

Microsoft

(MD-102)

Endpoint Administrator

prepdaxams.com

Total: **387 Questions**

Question: 1

HOTSPOT -

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4

Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
ADatum plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -
Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 2

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30

✓

The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
ADatum plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -

Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

Which devices are registered by using the Windows Autopilot deployment service?

A.Device1 only

B.Device3 only

C.Device1 and Device3 only

D.Device1, Device2, and Device3

Answer: A

Question: 3

HOTSPOT -

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -
The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.
Enterprise State Roaming is enabled for Group1 and GroupA.
Group1 and Group2 have a Membership type of Assigned.

Devices -
ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.
The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -
Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30

✓

The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4

Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
ADatum plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -
Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device5 marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 4

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA -

MAM user scope: GroupB -

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1 -

Folder protection: Enable -

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

Included groups: Group2, GroupB -

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
ADatum plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deployed a network boundary configuration profile that will have the following settings:

Name: Boundary1 -
Network boundary: 192.168.1.0/24

Scope tags: Tag1 -

Assignments:

Included groups: Group1, Group2 -

Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

Name: Connection1 -

Connection name: VPN1 -

Connection type: L2TP -

Assignments:

Included groups: Group1, Group2, GroupA

Excluded groups: --

Name: Connection2 -

Connection name: VPN2 -

Connection type: IKEv2 -

Assignments:

Included groups: GroupA -

Excluded groups: GroupB -

Technical Requirements -

ADatum must meet the following technical requirements:

Users in GroupA must be able to deploy new computers.

Administrative effort must be minimized.

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

A.Device2 only

B.Device3 only

C.Device1, Device2, and Device5 only

D.Device1, Device2, Device3, and Device4 only

Answer: D

Question: 5

HOTSPOT -

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

You have the iOS app protection policy shown in the following exhibit.

Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after /minutes of inactivity	30

Conditional launch

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

After 30 minutes of inactivity, a user will be prompted for their

account credentials only
PIN only
PIN and account credentials

Entering the wrong PIN five times will

block access
reset the app PIN
reset the device PIN
wipe company data

Answer:

Answer Area

After 30 minutes of inactivity, a user will be prompted for their

account credentials only
PIN only
PIN and account credentials

Entering the wrong PIN five times will

block access
reset the app PIN
reset the device PIN
wipe company data

Question: 6

DRAG DROP -

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11.

You need to create a customized installation of Microsoft 365 Apps for enterprise.

Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Actions

Run `setup.exe` and specify the `/packager` switch.

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

Edit the XML configuration file.

Run `setup.exe` and specify the `/download` switch.

Run `setup.exe` and specify the `/configure` switch.

Answer Area

1

2

3

4

Answer:

Actions

Run `setup.exe` and specify the `/packager` switch.

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

Edit the XML configuration file.

Run `setup.exe` and specify the `/download` switch.

Run `setup.exe` and specify the `/configure` switch.

Answer Area

1

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

2

Edit the XML configuration file.

3

Run `setup.exe` and specify the `/download` switch.

4

Run `setup.exe` and specify the `/configure` switch.

Question: 7

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

- A. Device2 only
- B. Device1 and Device2 only
- C. Device3 and Device4 only
- D. Device2, Device3, and Device4 only
- E. Device1, Device2, Device3, and Device4

Answer: C

Question: 8

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

All devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

▼

App configuration policy
App protection policy
Conditional access policy
Device compliance policy

Minimum number of policies:

▼

1
2
3
4
5

Answer:

Answer Area

Policy type:

▼

App configuration policy

App protection policy

Conditional access policy

Device compliance policy

Minimum number of policies:

▼

1

2

3

4

5

Question: 9

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

- A.the App1 deployment configurations
- B.a dynamic device group
- C.a detection rule
- D.the App2 deployment configurations

Answer: D

Question: 10

You have a Microsoft Intune subscription.

You have devices enrolled in Intune as shown in the following table.

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

- A.1
- B.2
- C.3
- D.4
- E.5

Answer: B

Question: 11

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune. Which extension should you select for the app package file?

- A..intunemac
- B..ipa
- C..apk
- D..appx

Answer: B

Question: 12

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named App1. App1 must only accept modern authentication requests.

You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

Assignments -

Users or workload identities: User1

Cloud apps or actions: App1 -

Access controls -

Grant: Block access -

You need to block only legacy authentication requests to App1.

Which condition should you add to CAPolicy1?

- A.Filter for devices
- B.Device platforms
- C.User risk
- D.Sign-in risk
- E.Client apps

Answer: E

Question: 13

HOTSPOT -

All users have Microsoft 365 apps deployed.

You need to configure Microsoft 365 apps to meet the following requirements:

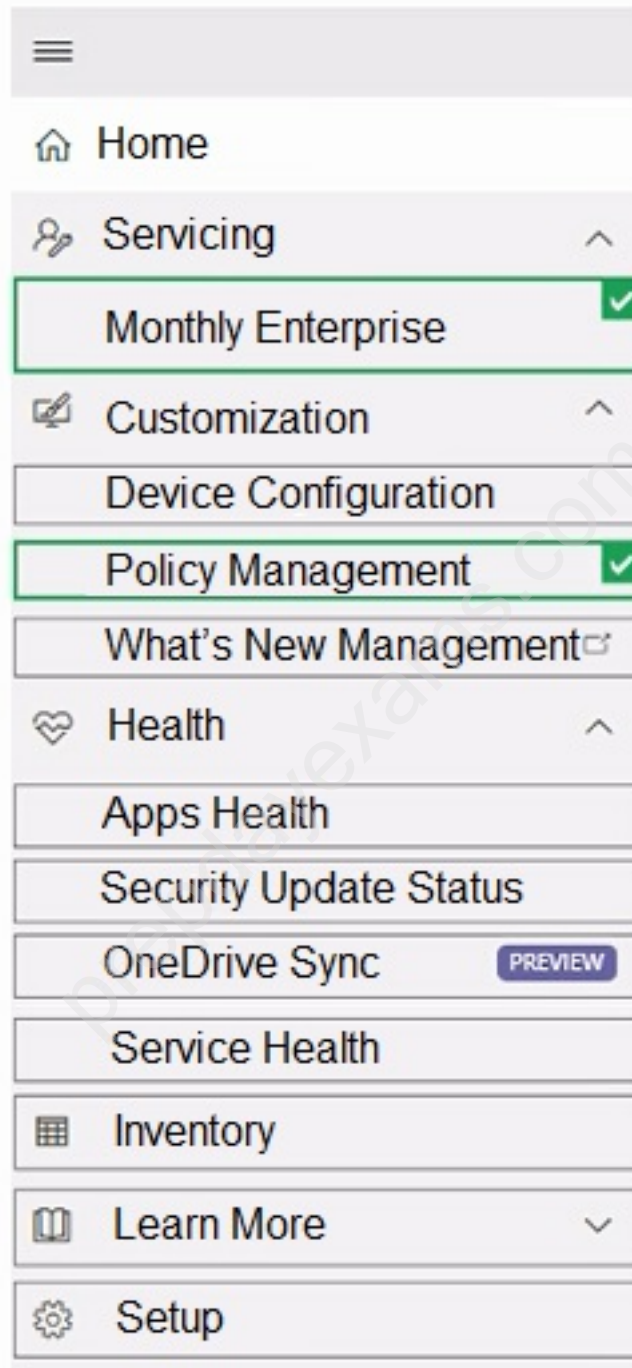
Enable the automatic installation of WebView2 Runtime.

Prevent users from submitting feedback.

Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.

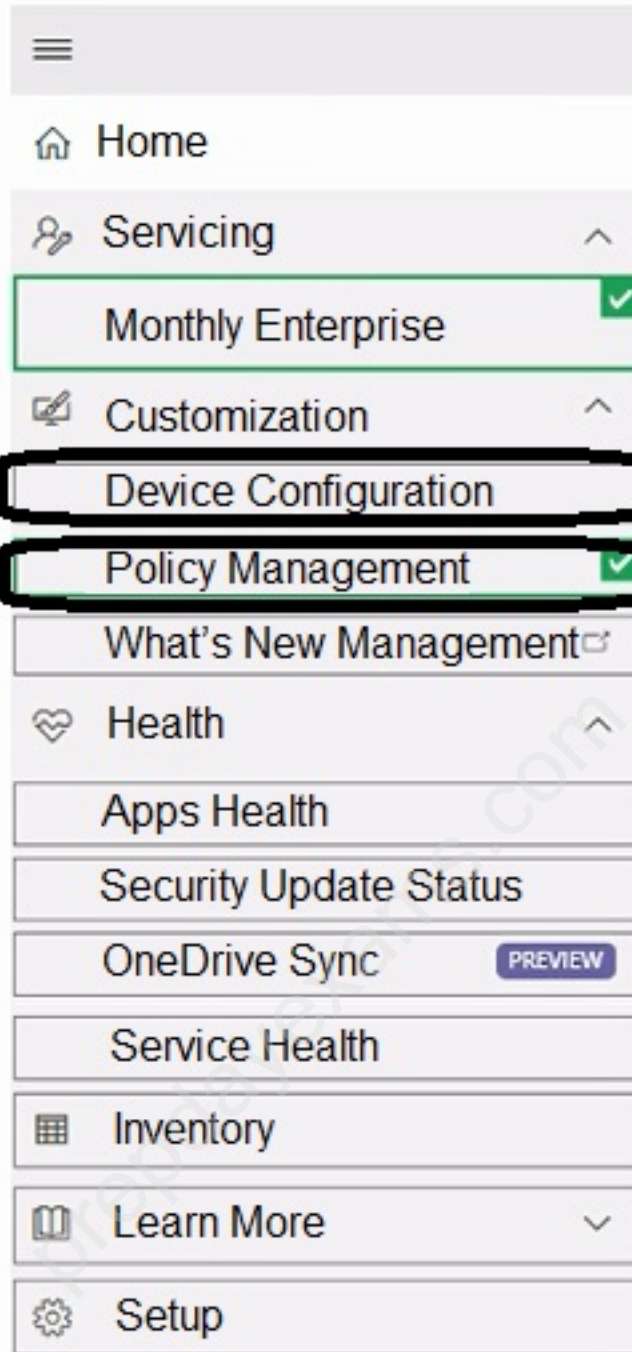
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 14

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).

You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.

What should you do?

- A.From the Microsoft Intune admin center, create a Windows 10 device profile.
- B.From Azure AD, add an app registration.
- C.From Azure AD, add an enterprise application.
- D.From the Microsoft Intune admin center, add an app.

Answer: D

Question: 15

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.

You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use?

- A.a Delete action
- B.a Retire action
- C.a Fresh Start action
- D.an Autopilot Reset action

Answer: A

Question: 16

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to review the startup times and restart frequencies of the devices.

What should you use?

- A.Azure Monitor
- B.Intune Data Warehouse
- C.Microsoft Defender for Endpoint
- D.Endpoint analytics

Answer: D

Question: 17

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings [Edit](#)

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**

▼

can be deferred indefinitely
can be deferred for 30 days
will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release

▼

1 day
30 days
60 days

Answer:

Answer Area

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**

▼

can be deferred indefinitely
can be deferred for 30 days
will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release

▼

1 day
30 days
60 days

Question: 18

You have computers that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from the Windows event logs. The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

- A.1 only
- B.2 and 3 only
- C.1 and 3 only
- D.1, 2, and 4 only
- E.1, 2, 3, and 4

Answer: D

Question: 19

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

- A.Users and Accounts
- B.General
- C.System security
- D.Device experience

Answer: D

Question: 20

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

- A.Onboard the macOS devices to the Microsoft Purview compliance portal.
- B.From the Microsoft Intune admin center, create a security baseline.
- C.Install Defender for Endpoint on the macOS devices.
- D.From the Microsoft Intune admin center, create a configuration profile.

Answer: D

Question: 21

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.

You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
- B.To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
- C.To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
- D.To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
- E.To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
- F.To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

Answer: DE

Question: 22

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2.

You create a device configuration profile named Profile1. You assign Profile1 to Group1.

You need to ensure that Profile1 applies to Device1 only.

What should you modify in Profile1?

- A.Assignments
- B.Settings
- C.Scope (Tags)
- D.Applicability Rules

Answer: A

Question: 23

DRAG DROP -

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

Enforces compliance for Defender for Endpoint by using Conditional Access

Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Features

Answer Area

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

An Intune connection

Enforces compliance:

Prevents suspicious scripts:

Answer:

Answer Area

Enforces compliance:

An Intune connection

Prevents suspicious scripts:

An attack surface reduction (ASR) rule

Question: 24

Your network contains an on-premises Active Directory domain and an Azure AD tenant. The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

You need to migrate the existing Default Domain Policy GPO settings to a device configuration profile. Which device configuration profile type template should you use?

- A.Administrative Templates
- B.Endpoint protection
- C.Device restrictions
- D.Custom

Answer: C

Question: 25

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace. Which three types of data can you collect from the computers by using Log Analytics? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A.failure events from the Security log
- B.the list of processes and their execution times
- C.the average processor utilization
- D.error events from the System log
- E.third-party application logs stored as text files

Answer: CDE

Question: 26

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune.

You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

- A.an attack surface reduction (ASR) policy
- B.a security baseline
- C.an endpoint detection and response (EDR) policy
- D.an account protection policy
- E.an antivirus policy

Answer: C

Question: 27

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune.

Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.From Platform Settings, set Android device administrator Personally Owned to Block.
- B.From Platform Settings, set Android Enterprise (work profile) to Allow.
- C.From Platform Settings, set Android device administrator Personally Owned to Allow.
- D.From Platform Settings, set Android device administrator to Block.

Answer: BD

Question: 28

HOTSPOT -

You have the device configuration profile shown in the following exhibit.

Kiosk ...

Windows 10 and later

- 1 Basics 2 Configuration settings 3 Assignments

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. [Learn more about Windows kiosk mode.](#)

Select a kiosk mode * ⓘ Single app, full-screen kiosk ▼

User logon type * ⓘ Auto logon (Windows 10, version 1803+) ▼

Application type * ⓘ Add Microsoft Edge browser ▼


This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. [Learn more about Microsoft Edge kiosk mode.](#)

Edge Kiosk URL * ⓘ https://contoso.com ✓

Microsoft Edge kiosk mode type ⓘ Public Browsing (inPrivate) ▼

Refresh browser after idle time ⓘ 5

Specify Maintenance Window for App Restarts * ⓘ Require Not configured

Maintenance Window Start Time MM/DD/YYYY  h:mm:ss A

Maintenance Window Recurrence ⓘ Daily (recommended) ▼

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Users [answer choice].
can access any URL
cannot view the address bar in Microsoft Edge
can only access URLs that include contoso.com
can only access URLs that start with https://contoso.com

Windows 10 and later devices can have [answer choice].
a single Microsoft Edge instance that has a single tab
a single Microsoft Edge instance that has multiple tabs
multiple Microsoft Edge instances that have multiple tabs
multiple Microsoft Edge instances that each has a single tab

Answer:

Answer Area

Users [answer choice]

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have [answer choice]

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Question: 29

HOTSPOT -

You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Delivery Optimization setting:

- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object:

- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

Answer:

Answer Area

Delivery Optimization setting:

▼

Bandwidth optimization type
Download mode
VPN peer caching

Intune object:

▼

A configuration profile
App configuration policies
Windows 10 and later quality updates
Windows 10 and later update rings

Question: 30

HOTSPOT -

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group1
Device3	iOS	Group2

From Intune, you create and send a custom notification named Notification1 to Group1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1 receives Notification1 on Device1.

☐☐

User2 receives Notification1 on Device2.

☐☐

User1 receives Notification1 on Device3.

☐☐

Answer:

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 receives Notification1 on Device3.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 31

You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse.
What should you use to create the report?

- A.the Company Portal app
- B.Endpoint analytics
- C.the Azure portal app
- D.Microsoft Power BI

Answer: D

Question: 32

You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.
What should you do first?

- A.Configure an Apple MDM push certificate.
- B.Add your user account as a device enrollment manager (DEM).
- C.Modify the enrollment restrictions.
- D.Upload a file that has the device identifiers for each iPad.

Answer: A

Question: 33

HOTSPOT -

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Azure AD. The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:
The configuration must be managed from a central location.

Internet traffic must be minimized.

Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows Update technology to use:

Windows Server Update Services (WSUS)
Microsoft Configuration Manager
Windows Update for Business

Manage the configuration by using:

A Group Policy object (GPO)
Microsoft Configuration Manager
Microsoft Intune

Manage the traffic by using:

Delivery Optimization
BranchCache
Peer cache

Answer:

Answer Area

Windows Update technology to use:

Windows Server Update Services (WSUS)
Microsoft Configuration Manager
Windows Update for Business

Manage the configuration by using:

A Group Policy object (GPO)
Microsoft Configuration Manager
Microsoft Intune

Manage the traffic by using:

Delivery Optimization
BranchCache
Peer cache

Question: 34

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune.

You need to configure Delivery Optimization on the devices to meet the following requirements:

Allow downloads from the internet and from other computers on the local network.

Limit the percentage of used bandwidth to 50.

What should you use?

- A.a configuration profile
- B.a Windows Update for Business Group Policy setting
- C.a Microsoft Peer-to-Peer Networking Services Group Policy setting
- D.an Update ring for Windows 10 and later profile

Answer: A

Question: 35

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10.

You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

- A.Group2 only
- B.Group1 and Group2 only
- C.Group2 and Group3 only
- D.Group1, Group2, and Group3

Answer: A

Question: 36

DRAG DROP -

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune.

You need to create a compliance policy that meets the following requirements:

Requires BitLocker Drive Encryption (BitLocker) on each device

Requires a minimum operating system version

Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings

Answer Area

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Requires BitLocker:

Requires a minimum operating system version:

Answer:

Answer Area

Requires BitLocker:

Device Health

Requires a minimum operating system version:

Device Properties

Question: 37

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have the Windows 11 devices shown in the following table.

Name	Member of	BitLocker Drive Encryption (BitLocker)
Device1	Group1	Enabled
Device2	Group1, Group3	Disabled
Device3	Group1, Group2	Enabled

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

Basics [Edit](#)

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings [Edit](#)

Device Health

Require BitLocker	Require
-------------------	---------

Actions for noncompliance [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags [Edit](#)

Default

Assignments [Edit](#)

Included groups

Group

Group1

Group3



Excluded groups

Group

Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

Device1 will have Policy assigned and will be marked as compliant.

☐☐

Device2 will have Policy assigned and will be marked as compliant.

☐☐

Device3 will have Policy assigned and will be marked as compliant.

☐☐

Answer:

Answer Area

Statements	Yes	No
Device1 will have Policy assigned and will be marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 will have Policy assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 38

DRAG DROP -

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings

Require BitLocker

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

Answer:

Answer Area

- Device1: Require Secure Boot to be enabled on the device.
- Device2: Prevent jailbroken devices from having corporate access.
- Device3: Prevent rooted devices from having corporate access.

Question: 39

DRAG DROP -

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices. Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliancy policy.

1

2

3

4



Answer:

Answer Area

1

Create a PowerShell discovery script and a JSON file.

2

Upload the PowerShell script to Intune.

3

Create and assign a custom compliancy policy.

4

Review the compliance dashboard for results.

Question: 40

DRAG DROP -

You have a computer that runs Windows 10 and contains two local users named User1 and User2.

You need to ensure that the users can perform the following actions:

User1 must be able to adjust the date and time.

User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1:

User2:

Answer:

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1:

Administrators

User2:

Administrators

Question: 41

HOTSPOT -

You have an Azure AD tenant named contoso.com.

You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD joined:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Registered in contoso.com:

▼
Device1 and Device2 only
Device2 and Device3 only
Device3 and Device4 only
Device2, Device3, and Device4 only
Device1, Device2, Device3, and Device4

Answer:

Answer Area

Azure AD joined:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Registered in contoso.com:

▼
Device1 and Device2 only
Device2 and Device3 only
Device3 and Device4 only
Device2, Device3, and Device4 only
Device1, Device2, Device3, and Device4

Question: 42

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using .

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1@contoso.com is a member of the local Administrators group on Computer1.

☐
☐

Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.

☐
☐

Admin2@contoso.com can install software on Computer1.

☐
☐

Answer:

Answer Area

Statements

Yes

No

User1@contoso.com is a member of the local Administrators group on Computer1.

☒
☐

Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.

☐
☒

Admin2@contoso.com can install software on Computer1.

☐
☒

Question: 43

Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.

You enable Windows PowerShell remoting on the computers.

You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.

To which group should you add Admin1?

- A.Access Control Assistance Operators
- B.Remote Desktop Users
- C.Power Users
- D.Remote Management Users

Answer: D

Question: 44

HOTSPOT -

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit. Profile1 will be deployed to Windows 10 devices.

Create profile

Windows PC

- ✓ Basics
- 2 Out-of-box experience (OOBE)**
- 3 Assignments
- 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ

User-Driven

Join to Azure AD as * ⓘ

Azure AD joined

Microsoft Software License Terms ⓘ

Show

Hide

i Important information about hiding license terms

Privacy settings ⓘ

Show

Hide

i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11

Hide change account options ⓘ

Show

Hide

User account type ⓘ

Administrator

Standard

Allow pre-provisioned deployment ⓘ

No

Yes

Language (Region) ⓘ

Operating system default

Automatically configure keyboard ⓘ

No

Yes

Apply device name template ⓘ

No

Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer Area

Users who deploy a device by using Profile1
[answer choice].

are prevented from modifying any desktop settings
can create additional local users on the device
can modify the desktop settings for all device users
can modify the desktop settings only for themselves

Users can configure the [answer choice]
during the deployment.

computer name
Cortana settings
keyboard layout

Answer:

Answer Area

Users who deploy a device by using Profile1
[answer choice].

are prevented from modifying any desktop settings
can create additional local users on the device
can modify the desktop settings for all device users
can modify the desktop settings only for themselves

Users can configure the [answer choice]
during the deployment.

computer name
Cortana settings
keyboard layout

Question: 45

HOTSPOT -

You have a server named Server1 and computers that run Windows 10. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 10 computers to Windows 11 by using the MDT deployment wizard.

You need create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On Server1:

Import the Deployment Image Servicing and Management (DISM) PowerShell module
Import the WindowsAutopilotIntune Windows Powershell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:

Windows 11 image and package only
Windows 11 image and task sequence only
Windows 11 image only
Windows 11 image, task sequence, and package

Answer:

Answer Area

On Server1:

Import the Deployment Image Servicing and Management (DISM) PowerShell module
Import the WindowsAutopilotIntune Windows Powershell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:

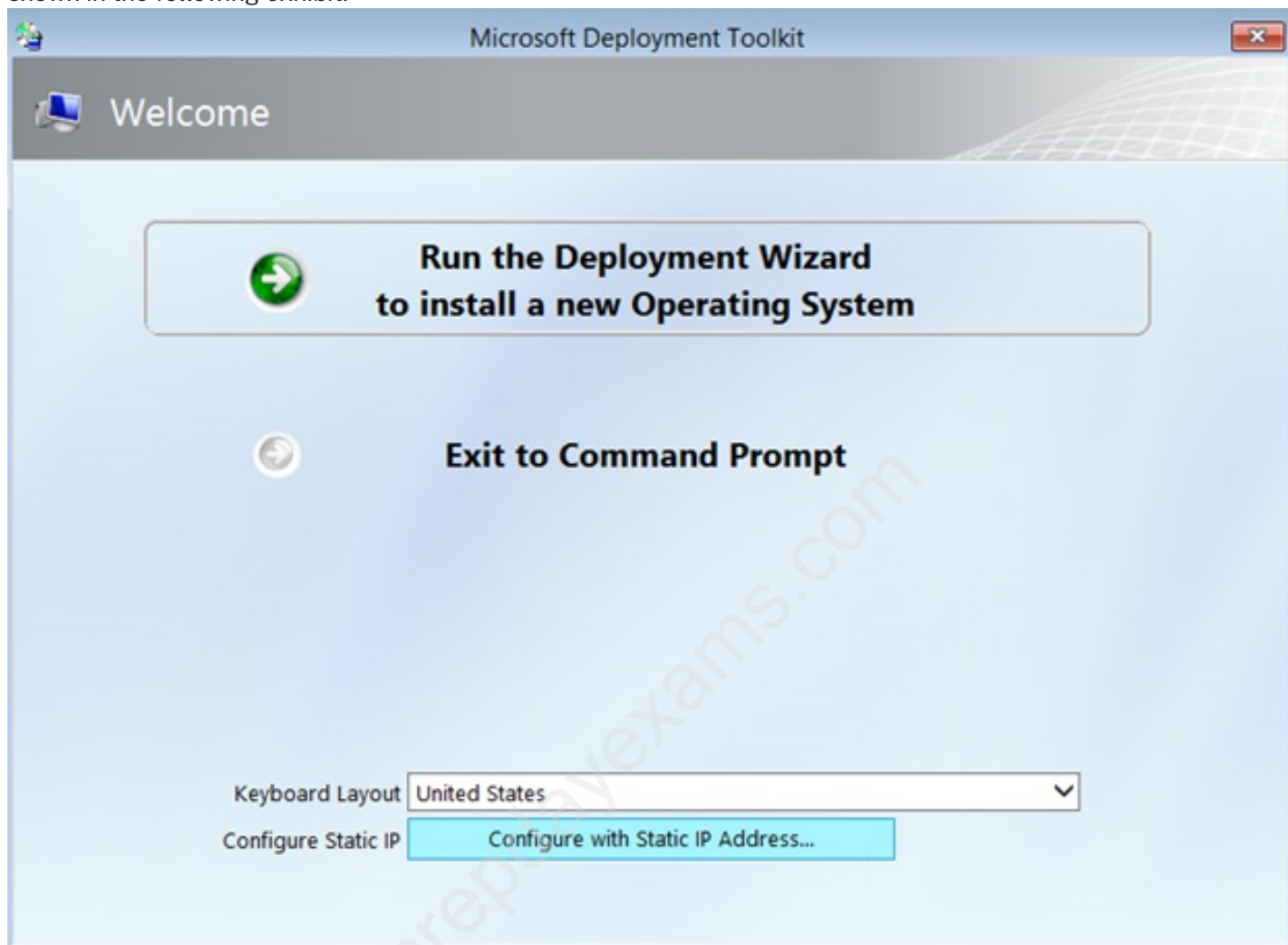
Windows 11 image and package only
Windows 11 image and task sequence only
Windows 11 image only
Windows 11 image, task sequence, and package

Question: 46

DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.



You need to prevent the welcome screen from appearing when the computers connect to MDT1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Modify the task sequence.

Replace the ISO image.

Modify the CustomSettings.ini file

Modify the Bootstrap.ini file

Update the deployment share.

Answer Area

1

2

3

Answer:

Actions

Modify the task sequence.

Replace the ISO image.

Modify the CustomSettings.ini file

Modify the Bootstrap.ini file

Update the deployment share.

Answer Area

1

Modify the Bootstrap.ini file

2

Modify the CustomSettings.ini file

3


Update the deployment share.

Question: 47

You use Windows Admin Center to remotely administer computers that run Windows 10. When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

The website's security certificate is not yet valid or has expired.

Error Code:

DLG_FLAGS_INVALID_CA

[Go on to the webpage](#) (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

- A.Client Authentication Issuers
- B.Personal
- C.Trusted Root Certification Authorities

Answer: C

Question: 48

HOTSPOT -

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 11	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure AD groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.

prepdaxams.com

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	--

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 49

HOTSPOT -

Your network contains an Active Directory domain. The domain contains 1,000 computers that run Windows 11. You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

Prevent the sharing of clipboard contents.

Ensure that users authenticate by using Network Level Authentication (NLA).

Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

▼	Remote Desktop Session Host	
	Connections	
	Device and Resource Redirection	
	Licensing	
	Printer Redirection	
	Profiles	
	RD Connection Broker	
▶	Remote Session Environment	✓
	Security	✓
	Session Time Limits	
	Temporary folders	

Answer:

Answer Area

▼	Remote Desktop Session Host	
	Connections	
	Device and Resource Redirection	
	Licensing	
	Printer Redirection	
	Profiles	
	RD Connection Broker	
▶	Remote Session Environment	✓
	Security	✓
	Session Time Limits	
	Temporary folders	

Question: 50

HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

Azure AD joined Windows devices enroll automatically in Intune.

You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications. Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows Autopilot:

▼

None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

In-place upgrade:

▼

None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

Answer:

Answer Area

Windows Autopilot:

None of the devices

Device1 only

Device1 and Device3 only

Device1, Device2, and Device3

In-place upgrade:

None of the devices

Device1 only

Device1 and Device3 only

Device1, Device2, and Device3

Question: 51

DRAG DROP -

You have 100 computers that run Windows 10.

You plan to deploy Windows 11 to the computers by performing a wipe and load installation.

You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Configure known folder redirection in Microsoft OneDrive.

Run `scanstate.exe`.

Run `loadstate.exe`.

Enable Enterprise State Roaming.

Create a system image Backup.

Deploy Windows 11.

Restore a system image backup.

1

2

3

Answer:

Answer Area

1

Run `scanstate.exe`.

2

Deploy Windows 11.

3

Run `loadstate.exe`.

Question: 52

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device. You need to ensure that when a deployment fails, the deployment logs can be collected. What should you configure?

- A.the automatic enrollment settings
- B.the Windows Autopilot deployment profile
- C.the enrollment status page (ESP) profile
- D.the device configuration profile

Answer: C

Question: 53

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You have a device named Device1 that is enrolled in Intune. You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A.Deploy the Remote Help app to Device1.
- B.Assign the Help Desk Operator role to User1.
- C.Assign the Intune Administrator role to User1.
- D.Assign a Microsoft 365 E5 license to User1.
- E.Rerun device onboarding on Device1.
- F.Assign the Remote Help add-on license to User1.

Answer: ABF

Question: 54

You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

- A.Image1 only
- B.Image2 only
- C.Image1 and Image2

Answer: B

Question: 55

HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.

You use Microsoft Intune and Configuration Manager to manage devices.

You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.

Devices for the sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to the homes of the sales department users.

Administrative effort must be minimized.

Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth point.

Answer Area

Sales:

▼

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Marketing:

▼

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Answer:

Answer Area

Sales:

▼

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Marketing:

▼

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

Question: 56

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1. In the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models. You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models. What should you do first?

- A.Import an OS package.
- B.Create a selection profile.
- C.Add a Gather task to the task sequence.
- D.Add a Validate task to the task sequence.

Answer: B

Question: 57

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

- A.Multipath I/O (MPIO)
- B.Multipoint Connector
- C.Windows Deployment Services (WDS)
- D.Windows Server Update Services (WSUS)

Answer: C

Question: 58

Your company standardizes on Windows 10 Enterprise for all users. Some users purchase their own computer from a retail store. The computers run Windows 10 Pro. You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following requirements: Ensure that any applications installed by the users are retained. Minimize user intervention. What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

- A.Windows Autopilot
- B.Microsoft Deployment Toolkit (MDT)
- C.a Windows Configuration Designer provisioning package
- D.Windows Deployment Services (WDS)

Answer: C

Question: 59

Note: This question is part of a series of questions that present the same scenario. Each question in the series

contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 60

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 61

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

A.Yes

B.No

Answer: A

Question: 62

Case study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

The network contains an Active Directory domain named contoso.com that is synced to Azure AD.

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	None	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned changes -

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
- Implement co-management for the computers.

Technical Requirements -

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

You need to meet the technical requirements for the iOS devices.

Which object should you create in Intune?

- A.a deployment profile
- B.an app protection policy
- C.a device configuration profile
- D.a compliance policy

Answer: C

Question: 63

HOTSPOT

-

Case study

-

Overview

-

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment

-

The network contains an Active Directory domain named contoso.com that is synced to Azure AD.

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration

-

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	<i>None</i>	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements

-

Planned changes

-

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and

were purchased already.

- Implement co-management for the computers.

Technical Requirements

-

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

You are evaluating which devices are compliant.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area		
Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 64

Case study -

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

The network contains an Active Directory domain named contoso.com that is synced to Azure AD.

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	None	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned changes -

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
- Implement co-management for the computers.

Technical Requirements -

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

You need to prepare for the deployment of the Phoenix office computers.

What should you do first?

- A.Generalize the computers and configure the Device settings from the Microsoft Entra admin center.
- B.Extract the serial number of each computer to an XML file and upload the file from the Microsoft Intune admin center.
- C.Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.
- D.Generalize the computers and configure the Mobility (MDM and MAM) settings from the Microsoft Entra admin center.
- E.Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune admin center.

Answer: C

Question: 65

HOTSPOT

-

Case study

-

Overview

-

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment

-

The network contains an Active Directory domain named contoso.com that is synced to Azure AD.

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four

numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration

-

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	None	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	Not applicable	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	Not applicable	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	Not applicable	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	None
Policy2	Group2	Group3
Policy3	Group1	None

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements

-

Planned changes

-

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
- Implement co-management for the computers.

Technical Requirements

-

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

User2 can enroll a maximum of:

	▼
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

Answer:

Answer Area

User1 can enroll a maximum of:

▼

5 devices

10 devices

15 devices

1,000 devices

An unlimited number of devices

User2 can enroll a maximum of:

▼

5 devices

10 devices

15 devices

1,000 devices

An unlimited number of devices

Question: 66

HOTSPOT

-

Case study

-

Overview

-

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG), and finance (FIN) departments.

Contoso recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from

home.

Existing Environment

-

The network contains an Active Directory domain named contoso.com that is synced to Azure AD.

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration

-

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	<i>None</i>	GroupB

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	<i>Not applicable</i>	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	<i>Not applicable</i>	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	<i>Not applicable</i>	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	<i>None</i>
Policy2	Group2	Group3
Policy3	Group1	<i>None</i>

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements

-

Planned changes

-

Contoso plans to implement the following changes:

- Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
- Implement co-management for the computers.

Technical Requirements

-

Contoso must meet the following technical requirements:

- Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
- Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
- Create a provisioning package for new computers in the HR department.
- Block iOS devices from sending diagnostic and usage telemetry data.
- Use the principle of least privilege whenever possible.
- Enable the users in the MKG department to use App1.
- Pilot co-management for the IT department.

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy1:

▼

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

Policy2:

▼

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

Answer:

Answer Area

Policy1:

▼

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

Policy2:

▼

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

Question: 67

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

On Computer1, you need to run the Invoke-Command cmdlet to execute several PowerShell commands on Computer2.

What should you do first?

- A. On Computer2, run the Enable-PSRemoting cmdlet.
- B. On Computer2, add Computer1 to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.
- D. On Computer1, run the New-PSSession cmdlet.

Answer: A

Question: 68

You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device2, Device3, and Device4

Answer: C

Question: 69

You have 25 computers that run Windows 10 Pro.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.

What should you use?

- A.Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
- B.Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
- C.Windows Autopilot
- D.Subscription Activation

Answer: D

Question: 70

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments.

From Deployment Workbench, you modify the WinPE settings and add PowerShell support.

You need to generate a new set of WinPE boot image files that contain the updated settings.

What should you do?

- A.From the Deployment Shares node, update the deployment share.
- B.From the Advanced Configuration node, create new media.
- C.From the Packages node, import a new operating system package.
- D.From the Operating Systems node, import a new operating system.

Answer: A

Question: 71

You are replacing 100 company-owned Windows devices.

You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:

- Back up the user state.
- Minimize administrative effort.

Which task sequence template should you use?

- A.Standard Client Task Sequence
- B.Standard Client Replace Task Sequence
- C.Litetouch OEM Task Sequence
- D.Sysprep and Capture

Answer: B

Question: 72

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11.

You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

- For the WinRM service, set Startup type to Automatic.
- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications.

Which PowerShell cmdlet should you use?

- A.Connect-WSMan
- B.Enable-PSRemoting
- C.Invoke-WSManAction
- D.Enable-PSSessionConfiguration

Answer: B

Question: 73

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Group1 and User2.

You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device2	Windows 10 Pro	Azure AD

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 74

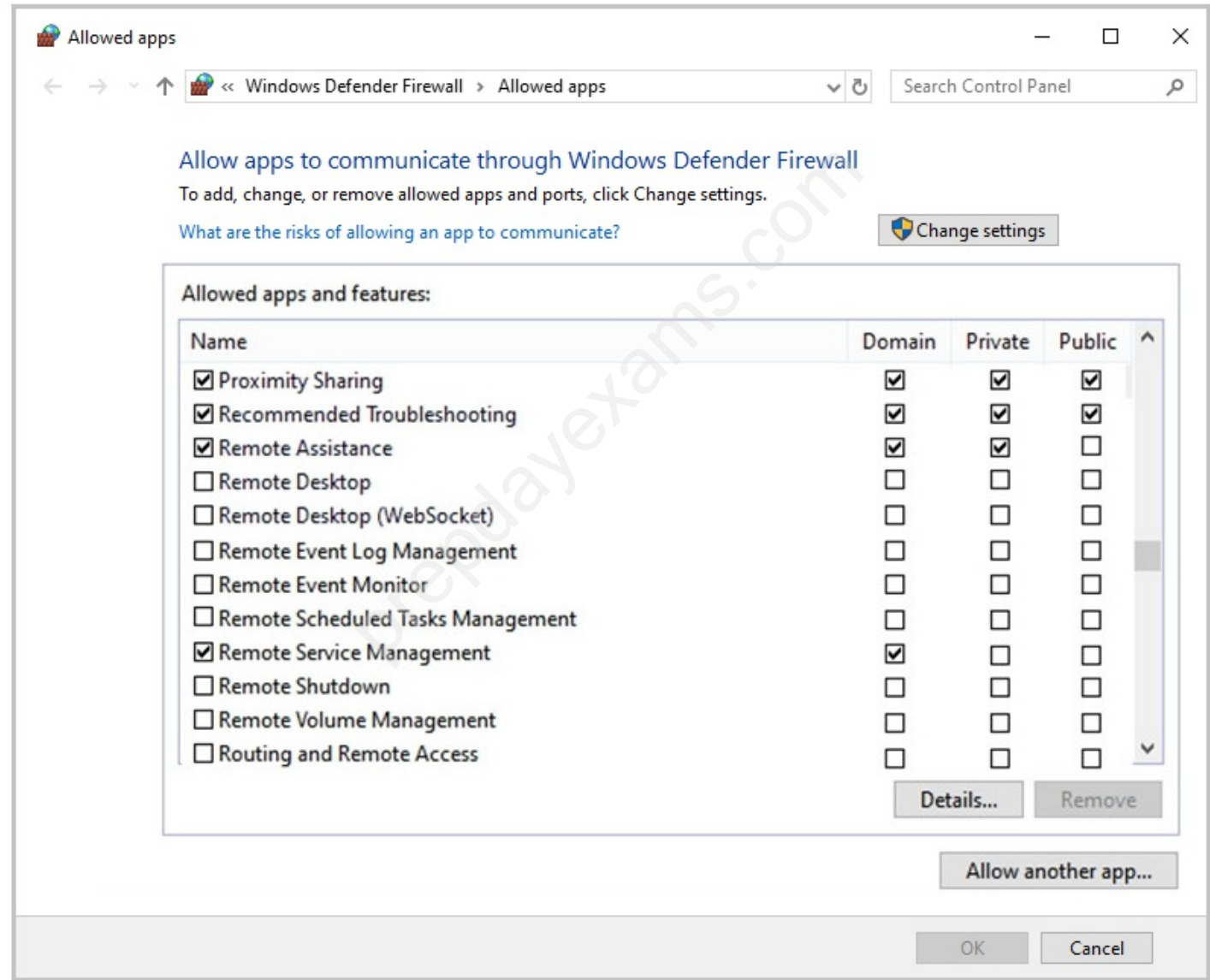
HOTSPOT

Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public

The local Administrator accounts on Computer1, Computer2, and Computer3 have the same user name and password.

On Computer1, Windows Defender Firewall is configured as shown in the following exhibit.



The services on Computer1 have the following states.

Status	Name	DisplayName
-----	-----	-----
Stopped	RasAuto	Remote Access Auto Connection Manager
Running	RasMan	Remote Access Connection Manager
Stopped	RemoteAccess	Routing and Remote Access
Stopped	RemoteRegistry	Remote Registry
Stopped	RetailDemo	Retail Demo Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Stopped	RpcLocator	Remote Procedure Call (RPC) Locator
Running	RpcSs	Remote Procedure Call (RPC)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="radio"/>	<input type="radio"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="radio"/>	<input type="radio"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="radio"/>	<input checked="" type="radio"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="radio"/>	<input checked="" type="radio"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 75

You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

- A.VM1 only
- B.VM3 only
- C.VM1 and VM2 only
- D.VM2 and VM3 only
- E.VM1, VM2, and VM3

Answer: B

Question: 76

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page.

You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 10 Home	Research
Device3	Windows 10	Marketing

You capture and upload the hardware IDs of the devices in the marketing department.

You configure Windows Autopilot.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can complete the Autopilot process on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 77

QUESTION NO: 77 -

You have a Microsoft 365 subscription that contains a user named User1. User1 is assigned a Windows 10/11 Enterprise E3 license.

You use Microsoft Intune Suite to manage devices.

User1 activates the following devices:

- Device1: Windows 11 Enterprise
- Device2: Windows 10 Enterprise
- Device3: Windows 11 Enterprise

How many more devices can User1 activate?

- A.2
- B.3

- C.7
- D.8

Answer: A

Question: 78

DRAG DROP

Your company has a computer named Computer1 that runs Windows 10.

Computer1 was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user.

You need to redeploy Computer1 by using Windows Autopilot.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Upload the file by using Microsoft Intune.

Generate a CSV file that contains the computer information.

Reset the computer.

Generate a JSON file that contains the computer information.

Upload the file by running `azcopy.exe`.

Answer Area

1

2

3

Answer:

Answer Area

Generate a CSV file that contains the computer information.

Upload the file by using Microsoft Intune.

Reset the computer.

Question: 79

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.

You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 Enterprise to new computers. The computers have a single hard disk.

You need to modify the task sequence to create a system volume and a data volume.

Which phase should you modify in the task sequence?

- A. Initialization
- B. State Restore
- C. Preinstall
- D. Postinstall

Answer: C

Question: 80

You have a Microsoft Deployment Toolkit (MDT) deployment share.

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



Select OS

General Settings

Select Template

Select OS

Specify Product Key

OS Settings


Admin Password

Summary

Progress

Confirmation

The following operating system images are available to be deployed with this task sequence. Select the one to use.

 Operating Systems

Previous

Next

Cancel

You need to be able to select an operating system image to perform a Windows 11 in-place upgrade.

What should you do?

- A.Enable monitoring for the deployment share.
- B.Import a full set of source files.
- C.Import a custom image file.
- D.Run the Update Deployment Share Wizard.

Answer: B

Question: 81

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection. The company's security policy states the following:

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.
- Users can use their personal iOS and Android devices to access corporate cloud services.
- Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

You need to configure a solution to enforce the security policy.

What should you create?

- A.a device configuration profile from the Microsoft Intune admin center
- B.a data loss prevention (DLP) policy from the Microsoft Purview compliance portal
- C.an insider risk management policy from the Microsoft Purview compliance portal
- D.an app protection policy from the Microsoft Intune admin center

Answer: D

Question: 82

You have a Microsoft 365 subscription that contains 500 Android Enterprise devices.

All the devices are enrolled in Microsoft Intune.

You need to deliver bookmarks to the Chrome browser on the devices.

What should you create?

- A.a compliance policy
- B.a configuration profile
- C.an app protection policy
- D.an app configuration policy

Answer: D

Question: 83

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.

You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).

What should you use to create a customization file for ODT?

- A.the Microsoft 365 admin center
- B.the Microsoft Intune admin center
- C.the Microsoft Purview compliance portal
- D.the Microsoft 365 Apps admin center

Answer: D

Question: 84

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to use Intune to deploy an application named App1 that contains multiple installation files.

What should you do first?

- A.Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.

- B.Create an Android application package (APK).
- C.Upload the contents of App1 to Intune.
- D.Install the Microsoft Deployment Toolkit (MDT).

Answer: A

Question: 85

HOTSPOT

-

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")


You are deploying Microsoft 365 apps.

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Intune admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App information

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	--
Logo	

App suite configuration [Edit](#)

Apps to be installed as part of the suite	Access Excel, OneNote, Outlook, PowerPoint, Publisher, Skype for Business, Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Terms on behalf of users	No
Install background service for Microsoft Search in Bing	Yes
Apps to be installed as part of the suite	1 language(s) selected

Assignments [Edit](#)

Group mode	Group
✓ Required	
⊕ Included	Group1
> Available for enrolled devices	

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
LT1 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>
LT2 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>
LT3 will have Microsoft 365 apps installed.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
LT1 will have Microsoft 365 apps installed.	<input checked="" type="radio"/>	<input type="radio"/>
LT2 will have Microsoft 365 apps installed.	<input type="radio"/>	<input checked="" type="radio"/>
LT3 will have Microsoft 365 apps installed.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 86

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

- A.a device restrictions device configuration profile
- B.an app configuration policy
- C.a Windows 10 and later security baseline
- D.a custom device configuration profile
- E.a Windows 10 and later update ring

Answer: DE

Question: 87

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

- A.Modify the Baseline regression threshold.
- B.Onboard 10 devices to Endpoint analytics.
- C.Create a Log Analytics workspace.
- D.Create an Azure Monitor workbook.

Answer: B

Question: 88

You install a feature update on a computer that runs Windows 10.

How many days do you have to roll back the update?

- A.5
- B.10
- C.14
- D.30

Answer: B

Question: 89

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.

You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

- A.Join Azure AD.
- B.Configure Windows Defender Firewall.
- C.Create an event subscription
- D.Install the Azure Monitor Agent.

Answer: A

Question: 90

You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a device configuration profile.
- B. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
- C. Create a compliance policy.
- D. Create an iOS app provisioning profile.
- E. Enroll the devices in Microsoft Intune by using Apple Business Manager.

Answer: AE

Question: 91

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRing1 that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time
- Automatic behavior frequency: First week of the month
- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1.

When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

Answer: B

Question: 92

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

You discover that Group Policy settings override the settings configured in Microsoft Intune policies.

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.

What should you do?

- A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
- B. From the Microsoft Intune admin center, create a custom device profile.

- C.From the Microsoft Intune admin center, create an Administrative Templates device profile.
- D.From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Answer: B

Question: 93

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

- A.the Azure Monitor agent
- B.a device compliance policy
- C.a Conditional Access policy
- D.an Intune data collection policy

Answer: D

Question: 94

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an iOS/iPadOS update profile as shown in the following exhibit.

Create profile ...

iOS/iPadOS

✓ Basics ✓ Configuration settings ✓ Scope tags ✓ Assignments **5** Review + create

Summary

Basics

Name Profile1

Description ..

Update policy settings

Update to install	Install iOS/iPadOS Latest update			
Schedule type	Update outside of scheduled time			
Time zone	UTC ±00			
Time window	Start day	Start time	End day	End time
	Monday	1 AM	Wednesday	1 PM
	Friday	1 AM	Saturday	11 PM

Assignments

Included groups

Group	Group Members ⓘ
Group1	3 devices, 0 users

Excluded groups

Group	Group Members ⓘ
Group2	1 devices, 0 users

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.

☐☐

If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.

☐☐

If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.

☐☐

Answer:

Answer Area

Statements

Yes

No

If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.

☒☐

If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.

☐☒

If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.

☐☒

Question: 95

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	<i>Not applicable</i>
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	<i>Not applicable</i>

You create a policy set named Set1 and add Comply1 to Set1.

Which additional resources can you add to Set1?

A.Conf1 only

B.Comply2 only

- C. Comply2 and Conf1 only
- D. CA1, Conf1, and Office1 only
- E. Comply2, CA1, Conf1, and Office1

Answer: C

Question: 96

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

- A. Microsoft Defender for Endpoint Power BI app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Answer: B

Question: 97

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.

You plan to integrate Intune with Microsoft Defender for Endpoint.

You need to establish a service-to-service connection between Intune and Defender for Endpoint.

Which settings should you configure in the Microsoft Intune admin center?

- A. Premium add-ons
- B. Connectors and tokens
- C. Tenant enrollment
- D. Microsoft Tunnel Gateway

Answer: B

Question: 98

DRAG DROP

-

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

From the Microsoft Intune admin center, configure enrollment restrictions.

From the Enterprise CA, configure certificate managers.

Obtain the root certificate.

From the Microsoft Intune admin center, create a trusted certificate configuration profile.

From the Microsoft Intune admin center, create a PKCS certificate configuration profile.

1

2

3

Answer:

Answer Area

Obtain the root certificate.

From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

Question: 99

Your company uses Microsoft Intune.

More than 500 Android and iOS devices are enrolled in the Intune tenant.

You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.

You need to ensure that the policies can target the devices based on their version of Android or iOS.

What should you configure first?

- A.groups that have dynamic membership rules in Azure AD
- B.Device categories in Intune
- C.Corporate device identifiers in Intune
- D.Device settings in Azure AD

Answer: A

Question: 100

DRAG DROP

-

You have 500 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR)

You need to configure a Windows 10 device that will be used to create a template file.

Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Protection areas

Answer Area

Account protection

App & browser control

Device security

Virus & threat protection

DEP:

Mandatory ASLR:

Answer:

Answer Area

DEP: App & browser control

Mandatory ASLR: App & browser control

Question: 101

You have an Azure AD tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11.

You need to add Computer1 to contoso.com.

What should you use?

A.dsregcmd.exe

- B.Computer Management
- C.netdom.exe
- D.the Settings app

Answer: D

Question: 102

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching.

Which authentication method should you use?

- A.Microsoft Authenticator
- B.voice calls
- C.FIDO2 security keys
- D.text messages

Answer: A

Question: 103

You use a Microsoft Intune subscription to manage iOS devices.

You configure a device compliance policy that blocks jailbroken iOS devices.

You need to enable Enhanced jailbreak detection.

What should you configure?

- A.the Compliance policy settings
- B.the device compliance policy
- C.a network location
- D.a configuration profile

Answer: B

Question: 104

DRAG DROP

-

You have a Microsoft 365 subscription that contains two users named User1 and User2.

You need to ensure that the users can perform the following tasks:

- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for nonadministrative users.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

Global Administrator

Helpdesk Administrator

Security Administrator

User Administrator

Answer Area

User1:

User2:

Answer:

Answer Area

User1:

User Administrator

User2:

Helpdesk Administrator

Question: 105

HOTSPOT

You have a Microsoft Intune subscription that has the following device compliance policy settings:

- Mark devices with no compliance policy assigned as: Compliant
- Compliance status validity period (days): 14

On January1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group1

On January 4, you create the following two device compliance policies:

- Name: Policy1
- Platform: Windows 10 and later

- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1

- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 106

HOTSPOT

-

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

The next day, you review the compliance status of the computers.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The compliance status of Computer1 is in grace period.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer2 is Compliant.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer3 is Not compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The compliance status of Computer1 is in grace period.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance status of Computer2 is Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance status of Computer3 is Not compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 107

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure the Authentication methods.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 108

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Main-enabled security group
Group4	Security group

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

- A.Group3 and Group4 only
- B.Group3, Group4, and Admin1 only
- C.Group1, Group2, and Group3 only
- D.Group1, Group2, Group3, and Group4 only
- E.Group1, Group2, Group3, Group4, and Admin1

Answer: C

Question: 109

HOTSPOT

-

You have an Azure AD tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of .

You join a Windows 11 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

▼
 net accounts
 net localgroup
 net user

Administrators /add "

▼
 AzureAD
 CONTOSO
 UPN

\user1@contoso.com"

Answer:

Answer Area

Administrators /add " \user1@contoso.com"

net accounts
net localgroup
net user

AzureAD
CONTOSO
UPN

Question: 110

You have a Microsoft 365 subscription.

You need to provide a user the ability Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A.Global Administrator
- B.Conditional Access Administrator
- C.Security Administrator
- D.Intune Administrator

Answer: B

Question: 111

HOTSPOT

-

In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	<i>Not applicable</i>	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ☐ Compliant ☒ Not Compliant

Enhanced jailbreak detection ☐ Enabled ☒ Disabled

Compliance status validity period (days) ☒

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 9, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On June 9, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 112

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices that run Windows 11.

User provides remote support for 75 devices in the marketing department.

You need to add User1 to the Remote Desktop Users group on each marketing department device.

What should you configure?

- A. an app configuration policy
- B. a device compliance policy
- C. an account protection policy
- D. a device configuration profile

Answer: C

Question: 113

HOTSPOT

-

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	License
User1	Group1	Microsoft 365 E5
User2	Group2	Microsoft 365 E5

For contoso.com, the Mobility (MDM and MAM) settings have the following configurations:

- MDM user scope: Group1
- MAM user scope: Group2

You purchase the devices shown in the following table:

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 114

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to deploy and manage Windows devices.

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

- A. Deploy a new configuration profile to the devices.
- B. Perform a Windows Autopilot reset on the devices.
- C. Perform an in-place upgrade on the devices.
- D. Perform a clean installation of Windows 11 on the devices.

Answer: B

Question: 115

HOTSPOT

-

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

- Automatically enroll new devices and provision system apps without requiring end-user authentication
- Include the hardware serial number in the computer name.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create profile

Windows PC

- ✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ	User-Driven	▼
Join to Azure AD as * ⓘ	Azure AD joined	▼
Microsoft Software License Terms ⓘ	Show	Hide
i Important information about hiding license terms		
Privacy settings ⓘ	Show	Hide
i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more		
Hide change account options ⓘ	Show	Hide
User account type ⓘ	Administrator	Standard
Allow pre-provisioned deployment ⓘ	No	Yes
Language (Region) ⓘ	Operating system default	▼
Automatically configure keyboard ⓘ	No	Yes
Apply device name template ⓘ	No	Yes

Answer:

Answer Area

Create profile

Windows PC

✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode *	User-Driven
Join to Azure AD as *	Azure AD joined
Microsoft Software License Terms	Show Hide
<i>i</i> Important information about hiding license terms	
Privacy settings	Show Hide
<i>i</i> The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more	
Hide change account options	Show Hide
User account type	Administrator Standard
Allow pre-provisioned deployment	No Yes
Language (Region)	Operating system default
Automatically configure keyboard	No Yes
Apply device name template	No Yes

Question: 116

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

- A. Turn on Reputation-based protection
- B. Enable Network Level Authentication (NLA)
- C. Turn on Network Discovery
- D. Configure the Remote Desktop Configuration service

Answer: B

Question: 117

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

- A.Device3 only
- B.Device2 and Device3 only
- C.Device1 and Device2 only
- D.Device1, Device2, and Device3

Answer: B

Question: 118

HOTSPOT

-

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2.

The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	Group3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 119

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled.

From Computer1, you connect to Computer2 by using Remote Desktop Connection.

You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.

What should you do?

- A.From Computer2, configure the Remote Desktop settings.
- B.From Windows Defender Firewall on Computer1, allow Remote Desktop.
- C.From Windows Defender Firewall on Computer2, allow File and Printer Sharing.
- D.From Computer1, configure the Remote Desktop Connection settings.

Answer: D

Question: 120

You have a Microsoft 365 subscription that uses Microsoft Intune.

You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A.subscription activation
- B.a custom Windows image
- C.an in-place upgrade
- D.Windows Autopilot
- E.provisioning packages

Answer: BDE

Question: 121

DRAG DROP

-

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

You import a Windows 11 image to DS1.

You have an executable installer for an application named App1.

You need to ensure that App1 will be installed for all the task sequences that deploy the image.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Modify a Windows 11 operating system setting.

Modify a selection profile.

Add App1 to DS1.

Identify the GUID of App1.

Modify CustomSettings.ini.

1

2

3



Answer:

Answer Area

1

Add App1 to DS1.

2

Identify the GUID of App1.

3

Modify CustomSettings.ini.

Question: 122

HOTSPOT

-

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Server1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Answer:

Answer Area

Device1:

LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Question: 123

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to configure the Out-of-box experience (OOBE) settings.

What should you create in the Microsoft Intune admin center?

- A.an enrollment status page (ESP)
- B.a deployment profile
- C.a compliance policy
- D.a PowerShell script
- E.a configuration profile

Answer: B

Question: 124

You have an Azure AD tenant that contains the devices shown in the following table.

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

You purchase Windows 11 Enterprise E5 licenses.

Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device2, Device3, and Device4

Answer: A

Question: 125

You have a Microsoft 365 Subscription that uses Microsoft Intune.

You add apps to Intune as shown in the following table.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform.

Which apps can you manage by using Policy1?

- A.App2 only
- B.App3 only
- C.App1 and App3 only
- D.App2 and App3 only
- E.App1, App2, and App3

Answer: B

Question: 126

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices.

What should you do first?

- A.Create a configuration profile.
- B.Add a certificate connector.
- C.Configure the Partner device management settings.
- D.Link your managed Google Play account to Intune.

Answer: D

Question: 127

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

NOTE: Each correct selection is worth one point.

- A.Privacy URL
- B.Information URL
- C.Developer
- D.Owner

Answer: AB

Question: 128

HOTSPOT

-

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Device restrictions

Windows 10 and later

✓ Basics **2 Configuration settings** ③ Assignments ④ Applicability Rules ⑤ Review + create

✓ App Store

✓ Cellular and connectivity

✓ Cloud and Storage

✓ Cloud Printer

✓ Control Panel and Settings

✓ Display

✓ General

✓ Locked Screen Experience

✓ Messaging

✓ Microsoft Edge Browser

✓ Network proxy

✓ Password

✓ Per-app privacy exceptions

✓ Personalization

✓ Printer

✓ Privacy

✓ Projection

Previous

Next

Answer:

Device restrictions

Windows 10 and later

✓ Basics **2 Configuration settings** ③ Assignments ④ Applicability Rules ⑤ Review + create

▼

App Store

▼

Cellular and connectivity

▼

Cloud and Storage

▼

Cloud Printer

▼

Control Panel and Settings

▼

Display

▼

General

▼

Locked Screen Experience

▼

Messaging

▼

Microsoft Edge Browser

▼

Network proxy

▼

Password

▼

Per-app privacy exceptions

▼

Personalization

▼

Printer

▼

Privacy

▼

Projection

Previous

Next

Question: 129

You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to upgrade the computers to Windows 11 Enterprise.

What should you configure in Intune?

- A.a device compliance policy
- B.a device cleanup rule
- C.a device enrollment policy
- D.a device configuration profile

Answer: D

Question: 130

You have computers that run Windows 10 and are managed by using Microsoft Intune.

Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1.

What should you configure in the device configuration profile?

- A. Microsoft Defender Exploit Guard
- B. Microsoft Defender Application Guard
- C. Microsoft Defender SmartScreen
- D. Microsoft Defender Application Control

Answer: A

Question: 131

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to meet the following requirements:

- Hide the Firewall & network protection area in the Windows Security app.
- Disable the provisioning of Windows Hello for Business on the devices.

Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Manage



Antivirus



Disk encryption



Firewall



Endpoint detection and response



Attack surface reduction



Account protection



Device compliance



Conditional access

Answer:

Answer Area

Manage



Antivirus



Disk encryption



Firewall



Endpoint detection and response



Attack surface reduction



Account protection



Device compliance



Conditional access

Question: 132

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune.

You need to review the startup processes and how often each device restarts.

What should you use?

- A. Endpoint analytics
- B. Device Management
- C. Azure Monitor
- D. Intune Data Warehouse

Answer: A

Question: 133

DRAG DROP

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to enforce the following requirements:

- Computers that run macOS must have FileVault enabled.
- Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled.
- Computers that run Windows 10 must have Microsoft Defender Application Control enabled.

Which Endpoint security feature should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Features

Answer Area

Account protection

Attack surface reduction (ASR)

Disk encryption

Endpoint detection and response (EDR)

Computers that run macOS must have FileVault enabled:

Computers that run Windows 10 must have Microsoft Defender Application Control enabled:

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:

Answer:

Answer Area

Computers that run macOS must have FileVault enabled:

Disk encryption

Computers that run Windows 10 must have Microsoft Defender Application Control enabled:

Attack surface reduction (ASR)

Computers that run Windows 10 must have Microsoft Defender Credential Guard enabled:

Account protection

Question: 134

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune.

Currently, Windows updates are downloaded without using Delivery Optimization.

You need to configure the computers to use Delivery Optimization.

What should you create in Intune?

- A.a device compliance policy
- B.a Windows 10 update ring
- C.a device configuration profile
- D.an app protection policy

Answer: C

Question: 135

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows 11 devices in Intune.

What should you use?

- A.a provisioning package
- B.a Group Policy Object (GPO)
- C.mobile device management (MDM) automatic enrollment
- D.a device configuration policy


Answer: A

Question: 136

HOTSPOT

-

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
 LON-CL2	✔ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✔ Yes
 LON-CL4	✔ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✔ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Identified by Intune as a personal device:

LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Answer:

Answer Area

Identified by Intune as a personal device:

LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Question: 137

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices. All devices are in the same time zone.

You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy.

All devices remain online.

Without further modification to the policy, on which date will the devices next attempt to update?

- A.December 1
- B.December 6
- C.November 15
- D.November 22

Answer: B

Question: 138

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Operating system	Enrolled in Microsoft Intune
Device1	Windows 11	Yes
Device2	Windows 10	Yes
Device3	Android	Yes
Device4	iOS	Yes

All devices have Microsoft Edge installed.

From the Microsoft Intune admin center, you create a Microsoft Edge Baseline profile named Edge1.

You need to apply Edge1 to all the supported devices.

To which devices should you apply Edge1?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1, Device2, and Device3 only
- D.Device1, Device2, and Device4 only
- E.Device1, Device2, Device3, and Device4

Answer: B

Question: 139

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to manage Windows updates by using Intune.

You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.

User experience settings

Automatic update behavior ⓘ	Auto install at maintenance time ▼
Active hours start * ⓘ	8 AM ▼
Active hours end * ⓘ	5 PM ▼
Restart checks ⓘ	<input checked="" type="button" value="Allow"/> <input type="button" value="Skip"/>
Option to pause Windows updates ⓘ	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>
Option to check for Windows updates ⓘ	<input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>
Change notification update level ⓘ	Use the default Windows Update notifications ▼
Use deadline settings ⓘ	<input checked="" type="button" value="Allow"/> <input type="button" value="Not configured"/>
Deadline for feature updates ⓘ	5 ✓
Deadline for quality updates ⓘ	2 ✓
Grace period ⓘ	1 ✓
Auto reboot before deadline ⓘ	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Automatic restarts are blocked
[answer choice].

▼

before 8 AM
between 8 AM and 5 PM
after 5 PM

A restart will be forced on a device
[answer choice] after the deadline.

▼

1 day
2 days
5 days

Answer:

Answer Area

Automatic restarts are blocked
[answer choice].

▼

before 8 AM

between 8 AM and 5 PM

after 5 PM

A restart will be forced on a device
[answer choice] after the deadline.

▼

1 day

2 days

5 days

Question: 140

You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy1 restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business.

What should you do?

- A.From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
- B.From the Microsoft Intune admin center, review Device compliance report.
- C.From the Microsoft Intune admin center, review the Noncompliant devices report.
- D.From the Microsoft Intune admin center, review the Setting compliance report.

Answer: A

Question: 141

HOTSPOT

-

You use Microsoft Intune to manage Windows 10 devices.

You are designing a reporting solution that will provide reports on the following:

- Compliance policy trends
- Trends in device and user enrollment
- App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Data source:

▼

Audit logs in Azure AD
Audit logs in Microsoft Intune
Azure Synapse Analytics
The Microsoft Intune Data Warehouse

Data visualization tool:

▼

Azure Data Studio
Microsoft Power BI
Microsoft Intune admin center

Answer:

Answer Area

Data source:

▼

Audit logs in Azure AD
Audit logs in Microsoft Intune
Azure Synapse Analytics
The Microsoft Intune Data Warehouse

Data visualization tool:

▼

Azure Data Studio
Microsoft Power BI
Microsoft Intune admin center

Question: 142

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10.

You implement hybrid Azure AD and Microsoft Intune.

You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort.

What should you use?

- A. an Autodiscover address record
- B. a Group Policy object (GPO)
- C. an Autodiscover service connection point (SCP)
- D. a Windows Autopilot deployment profile

Answer: B

Question: 143

HOTSPOT

-

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.

Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

You assign the update rings as shown in the following table.

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

Answer Area

Quality deferral on Computer1:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Quality deferral on Computer2:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Answer:

Answer Area

Quality deferral on Computer1:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Quality deferral on Computer2:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Question: 144

HOTSPOT

-

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to configure an Intune device configuration profile to meet the following requirements:

- Prevent Microsoft Office applications from launching child processes.
- Block users from transferring files over FTP.

Which two settings should you configure in the Endpoint protection configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Endpoint protection

Windows 10 and later

✓ Basics **2 Configuration settings** ③ Scope tags ④ Assignments ⑤ Applicability Rules ⑥ Review + create

✓ Microsoft Defender Application Guard

✓ Microsoft Defender Firewall

✓ Microsoft Defender SmartScreen

✓ Windows Encryption

✓ Microsoft Defender Exploit Guard

✓ Microsoft Defender Application Control

✓ Microsoft Defender Credential Guard

✓ Microsoft Defender Security Center

✓ Local device security options

✓ Xbox services

Answer:

Answer Area

Endpoint protection

Windows 10 and later

✓ Basics ② Configuration settings ③ Scope tags ④ Assignments ⑤ Applicability Rules ⑥ Review + create

- ▼ Microsoft Defender Application Guard
- ▼ Microsoft Defender Firewall
- ▼ Microsoft Defender SmartScreen
- ▼ Windows Encryption
- ▼ Microsoft Defender Exploit Guard
- ▼ Microsoft Defender Application Control
- ▼ Microsoft Defender Credential Guard
- ▼ Microsoft Defender Security Center
- ▼ Local device security options
- ▼ Xbox services

Question: 145

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

- A.Windows 10 only
- B.Windows 10 and Android only
- C.Windows 10 and iOS only
- D.Android and iOS only
- E.Windows 10, Android, and iOS

Answer: E

Question: 146

You are creating a device configuration profile in Microsoft Intune.

You need to configure specific OMA-URI settings in the profile.

Which profile type template should you use?

- A.Device restrictions (Windows 10 Team)
- B.Identity protection
- C.Custom
- D.Device restrictions

Answer: C

Question: 147

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of
User1	Group1
User2	<i>None</i>
User3	<i>None</i>

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.)

Device management [Edit](#)

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Profile Type
CompliancePolicy1	Windows 10 and later	Windows 10 and later co...

Device enrollment [Edit](#)

Windows autopilot deployment profiles

No results

Enrollment status pages

No results.

Assignments [Edit](#)

Included groups

All Users

Excluded groups

Group1

You enroll devices in Intune as shown in the following table.

Name	Operating system	User
Device1	Windows 10	User1
Device2	Windows 11	User2
Device3	Android	User3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 148

HOTSPOT

-

You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:

- Two hundred devices are enrolled by using the Intune Company Portal.
- Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).

You create an iOS/iPadOS software updates policy named Policy1 that is configured to install iOS/iPadOS 15.5.

How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of devices:

	▼
200	
800	
1000	

Configure a:

	▼
Compliance policy	
Conditional Access policy	
Device restriction policy	

Answer:

Answer Area

Number of devices:

	▼
200	
800	
1000	

Configure a:

	▼
Compliance policy	
Conditional Access policy	
Device restriction policy	

Question: 149

HOTSPOT

-

Case study

-

Overview

-

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment

-

Network Environment

-

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups

-

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices

-

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration


-


Microsoft Intune has the compliance policies shown in the following table.



Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as  Compliant Not Compliant

Enhanced jailbreak detection  Enabled Disabled

Compliance status validity period (days)  30 

The Automatic Enrollment settings have the following configurations:

- MDM user scope: GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: C:*\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments:
 - Included groups: Group2, GroupB

Windows Autopilot Configuration

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.

The Intune connector for Active Directory is installed on Server1.

Requirements

-

Planned Changes

-

ADatum plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
- Deployed a network boundary configuration profile that will have the following settings:
 - Name: Boundary1
 - Network boundary: 192.168.1.0/24
 - Scope tags: Tag1
 - Assignments:
 - Included groups: Group1, Group2
- Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
 - Name: Connection1
 - Connection name: VPN1
 - Connection type: L2TP
 - Assignments:
 - Included groups: Group1, Group2, GroupA
 - Excluded groups: --
 - Name: Connection2
 - Connection name: VPN2
 - Connection type: IKEv2
 - Assignments:
 - Included groups: GroupA
 - Excluded groups: GroupB

Technical Requirements

-

ADatum must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 150

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

- MDM user scope: GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: C:*\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments:
 - Included groups: Group2, GroupB

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4

Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.

The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.

•Deployed a network boundary configuration profile that will have the following settings:

- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:

- Included groups: Group1, Group2

•Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:

- Name: Connection1

- Connection name: VPN1

- Connection type: L2TP

- Assignments:

- Included groups: Group1, Group2, GroupA

- Excluded groups: --

- Name: Connection2

- Connection name: VPN2

- Connection type: IKEv2

- Assignments:

- Included groups: GroupA

- Excluded groups: GroupB

Technical Requirements -

ADatum must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.

To what should you grant the right to create the computer objects?

A.Server1

B.DC1

C.GroupA

D.Server2

Answer: A

Question: 151

HOTSPOT

-

Case study

-

Overview

-

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment

-

Network Environment

-

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups

-

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices

-

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration


-


Microsoft Intune has the compliance policies shown in the following table.



Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as  Compliant Not Compliant

Enhanced jailbreak detection  Enabled Disabled

Compliance status validity period (days)  30 

The Automatic Enrollment settings have the following configurations:

- MDM user scope: GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: C:*\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments:
 - Included groups: Group2, GroupB

Windows Autopilot Configuration

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4

Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.

The Intune connector for Active Directory is installed on Server1.

Requirements

-

Planned Changes

-

ADatum plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
- Deployed a network boundary configuration profile that will have the following settings:
 - Name: Boundary1
 - Network boundary: 192.168.1.0/24
 - Scope tags: Tag1
 - Assignments:
 - Included groups: Group1, Group2
- Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
 - Name: Connection1
 - Connection name: VPN1
 - Connection type: L2TP
 - Assignments:
 - Included groups: Group1, Group2, GroupA
 - Excluded groups: --
 - Name: Connection2
 - Connection name: VPN2
 - Connection type: IKEv2
 - Assignments:
 - Included groups: GroupA
 - Excluded groups: GroupB

Technical Requirements

-

ADatum must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

Answer Area

Device1:

	▼
1	
2	
3	
4	
5	

Device2:

	▼
1	
2	
3	
4	
5	

Answer:

Answer Area

Device1:

▼

1

2

3

4

5

Device2:

▼

1

2

3

4

5

Question: 152

Case study -

Overview -

ADatum Corporation is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

ADatum has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

The network contains an on-premises Active Directory domain named adatum.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

ADatum has a hybrid Azure AD tenant named adatum.com.

Users and Groups -

The adatum.com tenant contains the users shown in the following table.

Name	Azure AD role	Member of
User1	Cloud Device Administrator	GroupA
User2	Azure AD Joined Device Local Administrator	GroupB
User3	Global Reader	GroupA, GroupB
User4	Global Administrator	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

ADatum has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Intune Configuration -

Microsoft Intune has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30



The Automatic Enrollment settings have the following configurations:

- MDM user scope: GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: C:*\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments:
 - Included groups: Group2, GroupB

Windows Autopilot Configuration -

ADatum has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4 Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Windows Autopilot.

The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -

ADatum plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.

- Deployed a network boundary configuration profile that will have the following settings:
 - Name: Boundary1
 - Network boundary: 192.168.1.0/24
 - Scope tags: Tag1
 - Assignments:
 - Included groups: Group1, Group2
- Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
 - Name: Connection1
 - Connection name: VPN1
 - Connection type: L2TP
 - Assignments:
 - Included groups: Group1, Group2, GroupA
 - Excluded groups: --
 - Name: Connection2
 - Connection name: VPN2
 - Connection type: IKEv2
 - Assignments:
 - Included groups: GroupA
 - Excluded groups: GroupB

Technical Requirements -

ADatum must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

Which user can enroll Device6 in Intune?

- A.User4 and User1 only
- B.User4 and User2 only
- C.User4, User1, and User2 only
- D.User1, User2, User3, and User4

Answer: A

Question: 153

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune.

You need to prevent the printing of corporate data from managed apps on the devices.

What should you configure?

- A.an app configuration policy
- B.a security baseline
- C.an app protection policy
- D.an iOS app provisioning profile

Answer: C

Question: 154

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Application Administrator
Admin2	Cloud Application Administrator
Admin3	Office Apps Administrator
Admin4	Security Administrator

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization.

Which users can download the Office customization file from the admin center?

- A.Admin3 only
- B.Admin1 and Admin3 only
- C.Admin3 and Admin4 only
- D.Admin1, Admin2, and Admin3 only
- E.Admin1, Admin2, Admin3, Admin4

Answer: C

Question: 155

You have a Microsoft 365 E5 subscription.

You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.

What should you select in the Microsoft Intune admin center?

- A.Reports, and then Device compliance
- B.Apps, and then App protection policies
- C.Devices, and then Monitor
- D.Apps, and then Monitor

Answer: D

Question: 156

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group3	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1.

To which objects can you assign App1?

- A.Group3 and Group4 only
- B.Admin1, Group3, and Group4 only
- C.Group1, Group3, and Group4 only
- D.Group1, Group2, Group3, and Group4 only
- E.Admin1, Group1, Group2, Group3, and Group4

Answer: C

Question: 157

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android device named Policy1 as shown in the following exhibit.

[Home](#) > [Apps](#) >

Create policy

- ✓ Basics
- 2 Apps**
- 3 Data protection
- 4 Access requirements
- ...

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types ⓘ

No

Yes

Device types ⓘ

Unmanaged

Target policy to

All Apps

i We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

To apply Policy1 to an Android device, you must

▼

install the Company Portal app on the device
install the Microsoft Authenticator app on the device
onboard the device to Microsoft Defender for Endpoint
onboard the device to the Microsoft Purview compliance portal

When Policy1 is assigned, the policy will apply to

▼

users only
devices only
users and devices

Answer:

Answer Area

To apply Policy1 to an Android device, you must

▼

install the Company Portal app on the device
install the Microsoft Authenticator app on the device
onboard the device to Microsoft Defender for Endpoint
onboard the device to the Microsoft Purview compliance portal

When Policy1 is assigned, the policy will apply to

▼

users only
devices only
users and devices

Question: 158

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.From the Intune Company Portal, download App1.
- B.Sync App1 with Intune.
- C.From the Managed Google Play Store, approve App1.
- D.Create an OEMConfig profile.

Answer: BC

Question: 159

You have the Windows 10 devices shown in the following table.

Name	Operating system	Edition
Device1	64-bit version of Windows 10	Home
Device2	32-bit version of Windows 10	Pro
Device3	64-bit version of Windows 10	Enterprise
Device4	64-bit version of Windows 10	Pro

You plan to upgrade the devices to Windows 11 Enterprise.

On which devices can you perform a direct in-place upgrade to Windows 11 Enterprise?

- A.Device3 only
- B.Device3 and Device 4 only
- C.Device2, Device3, and Device4 only
- D.Device1, Device3, and Device4 only
- E.Device1, Device2, Device3, and Device4 only

Answer: B

Question: 160

HOTSPOT

-

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD.

A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1.

You need to identify what will occur when User1 next signs in to the devices.

What should you identify for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Device2:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Answer:

Answer Area

Device1:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Device2:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Question: 161

HOTSPOT

-

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1.

You add Windows 10 images to Share1 as shown in the following table.

Name	In WIM file	Description
Image1	Install1.wim	Default Windows 10 Pro image from the Windows 10 installation media
Image2	Install1.wim	Default Windows 10 Enterprise image from the Windows 10 installation media
Image3	Install2.wim	Default Windows 10 Pro for Workstations image from the Windows 10 installation media
Image4	Custom1.wim	Custom Windows 10 Enterprise image without any additional applications
Image5	Custom2.wim	Custom Windows 10 Enterprise image that includes custom applications

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence?

NOTE: Each correct selection is worth one point.

Answer Area

Standard Client Task Sequence:

▼

Image3 only

Image3, Image4, and Image5 only

Image1, Image2, and Image3 only

Image1, Image2, Image3, and Image4 only

Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

▼

Image3 only

Image3, Image4, and Image5 only

Image1, Image2, and Image3 only

Image1, Image2, Image3, and Image4 only

Image1, Image2, Image3, Image4, and Image5

Answer:

Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Question: 162

DRAG DROP

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to meet the following requirements during device provisioning:

- Display the progress of app and profile deployments.
- Join the devices to Azure AD.

What should you configure to meet each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings

Answer Area

CNAME Validation

Co-management Settings

Deployment Profiles

Enrollment notifications

Enrollment Status Page

Display the progress of app
and profile deployments:

Join the devices to Azure AD:

Answer:

Answer Area

Display the progress of app and profile deployments:

Enrollment Status Page

Join the devices to Azure AD:

Deployment Profiles

Question: 163

Your company has a Remote Desktop Gateway (RD Gateway).

You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.

You need to configure a Remote Desktop connection to connect through the gateway.

Which setting should you configure?

- A.Connect from anywhere
- B.Server authentication
- C.Connection settings
- D.Local devices and resources

Answer: A

Question: 164

You have a Microsoft Deployment Toolkit (MDT) deployment share.

You plan to deploy Windows 11 by using the Standard Client Task Sequence template.

You need to modify the task sequence to perform the following actions:

- Format disks to support Unified Extensible Firmware Interface (UEFI).
- Create a recovery partition.

Which phase of the task sequence should you modify?

- A.Preinstall
- B.PostInstall
- C.Install
- D.Initialization

Answer: A

Question: 165

DRAG DROP

Your network contains an Active Directory domain.

You install the Microsoft Deployment Toolkit (MDT) on a server.

You have a custom image of Windows 11.

You need to deploy the image to 100 devices by using MDT.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Enable multicast.

Install Windows Deployment Services (WDS).

Create a deployment share.

Add the Windows 11 image.

Create a task sequence.

Answer Area

1

2

3

Answer:

Answer Area

1

Create a deployment share.

2

Add the Windows 11 image.

3

Create a task sequence.

Question: 166

You have the Microsoft Deployment Toolkit (MDT) installed.

You install and customize Windows 11 on a reference computer.

You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.

Which command should you run before you capture the image?

- A.dism
- B.wpeinit
- C.sysprep
- D.bcdedit

Answer: C

Question: 167

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

You install Windows Admin Center on Computer1.

You need to manage Computer2 from Computer1 by using Windows Admin Center.

What should you do on Computer2?

- A.Update the TrustedHosts list.
- B.Run the Enable-PSRemoting cmdlet.
- C.Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
- D.Add an inbound Microsoft Defender Firewall rule.

Answer: B

Question: 168

HOTSPOT

-

You have a hybrid Azure AD tenant.

You configure a Windows Autopilot deployment profile as shown in the following exhibit.

Create profile ...

Windows PC

- 1 Basics 2 **Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ	User-Driven
Join to Azure AD as * ⓘ	Azure AD joined
Microsoft Software License Terms ⓘ	Show Hide
ⓘ Important information about hiding license terms	
Privacy settings ⓘ	Show Hide
ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.	
Hide change account options ⓘ	Show Hide
User account type ⓘ	Administrator Standard
Allow pre-provisioned deployment ⓘ	No Yes
Language (Region) ⓘ	Operating system default
Automatically configure keyboard ⓘ	No Yes
Apply device name template ⓘ	No Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

To apply the profile to a new computer, you must first

▼

join the device to Azure AD
enroll the device in Microsoft Intune
import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be

▼

joined to Azure AD only
registered in Azure AD only
joined to Active Directory only
joined to Active Directory and registered in Azure AD

Answer:

Answer Area

To apply the profile to a new computer, you must first

join the device to Azure AD
enroll the device in Microsoft Intune
import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be

joined to Azure AD only
registered in Azure AD only
joined to Active Directory only
joined to Active Directory and registered in Azure AD

Question: 169

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You plan to create Windows 11 device builds for the marketing and research departments. The solution must meet the requirements:

- Marketing department devices must support Windows Update for Business.
- Research department devices must have support for feature update versions for up to 36 months from release.

What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Marketing:

Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Research:

Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Answer:

Answer Area

Marketing:

▼

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

Research:

▼

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

Question: 170

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

- A. Device2 only
- B. Device3 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3

Answer: B

Question: 171

HOTSPOT

-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to deploy new Windows devices.

You plan to create a deployment profile.

You need to ensure that the deployment meets the following requirements:

- Devices must be joined to AD DS regardless of their current working location.
- Users in the marketing department must have a line-of-business (LOB) app installed during the deployment.

The solution must minimize administrative effort.

What should you do for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Devices must be joined to AD DS regardless of their current working location:

Deploy Always On VPN.
Install the Intune connector for Active Directory.
Modify the Autopilot deployment profile.
Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

Modify the Autopilot deployment profile.
Create a Microsoft Intune app deployment.
Create a device configuration profile in Intune.

Answer:

Answer Area

Devices must be joined to AD DS regardless of their current working location:

Deploy Always On VPN.
Install the Intune connector for Active Directory.
Modify the Autopilot deployment profile.
Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

Modify the Autopilot deployment profile.
Create a Microsoft Intune app deployment.
Create a device configuration profile in Intune.

Question: 172

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.Enable the Allow Remote Shell access setting.
- B.Enable the Allow remote server management through WinRM setting.

- C.Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
- D.Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
- E.Set the Startup Type of the Remote Registry service to Automatic.
- F.Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Answer: BCF

Question: 173

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.

You purchase a Microsoft 365 E5 subscription.

You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

- A.Windows Autopilot
- B.a Microsoft Deployment Toolkit (MDT) lite-touch deployment
- C.Subscription Activation
- D.an in-place upgrade by using Windows installation media

Answer: C

Question: 174

HOTSPOT

-

You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.

In Intune, you create a device compliance location that has the following configurations:

- Name: Network1
- IPv4 range: 192.168.0.0/16

In Intune, you create a device compliance policy for the Android platform. The policy has the following configurations:

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately
- Assigned: Group1

The Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 175

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
- Ensure that users can access company data seamlessly from their personal devices.
- Ensure that users can only sign in to their personal devices by using their personal account.

What should you use to add the devices to Azure AD?

A.Azure AD registered

- B.hybrid Azure AD join
- C.Azure AD joined

Answer: A

Question: 176

HOTSPOT

-

You have a Microsoft 365 subscription.

All computers are enrolled in Microsoft Intune.

You have business requirements for securing your Windows 11 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Requirement1:

▼

A conditional access policy
A device compliance policy
A device configuration profile

Requirement2:

▼

A conditional access policy
A device compliance policy
A device configuration profile

Answer:

Answer Area

Requirement1:

A conditional access policy
A device compliance policy
A device configuration profile

Requirement2:

A conditional access policy
A device compliance policy
A device configuration profile

Question: 177

HOTSPOT

-

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

- The members of Group1 must manage Intune roles and assignments.
- The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1:

	▼
Help Desk Operator	
Intune Role Administrator	
Intune Service Administrator	
Policy and Profile Manager	

Group2:

	▼
Help Desk Operator	
Intune Role Administrator	
Intune Service Administrator	
Policy and Profile Manager	

Answer:

Answer Area

Group1:

	▼
Help Desk Operator	
Intune Role Administrator	
Intune Service Administrator	
Policy and Profile Manager	

Group2:

	▼
Help Desk Operator	
Intune Role Administrator	
Intune Service Administrator	
Policy and Profile Manager	

Question: 178

HOTSPOT

-

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	<i>Not applicable</i>	Group3

Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	<i>Not applicable</i>

The device compliance policies has the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	Group3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 179

HOTSPOT

-

You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.

Intune has the device compliance policies shown in the following table.

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.)



Compliance policies | Compliance policy settings

...



Save Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as

☒ Compliant

Enhanced jailbreak detection

☐ Disabled

Compliance status validity period (days)

30

*

You create the following Conditional Access policy:

- Name: Policy1
- Assignments
 - o Users and groups: User1
 - o Cloud apps or actions: Office 365 SharePoint Online
- Access controls
 - o Grant: Require device to be marked as compliant
- Enable policy: On

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 180

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

- A.Windows Autopilot
- B.provisioning packages for Windows
- C.Security defaults in Azure AD
- D.Device settings in Azure AD

Answer: D

Question: 181

Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Intune admin center, you define the company's network as a location named Location1.

Which devices can use network location-based compliance policies?

- A.Device1 only
- B.Device2 only
- C.Device1 and Device2 only
- D.Device2 and Device3 only
- E.Device1, Device2, and Device3

Answer: E

Question: 182

You have an Azure subscription.

You have an on-premises Windows 11 device named Device1.

You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription.

To what should you associate DCR1?

- A.Azure Network Watcher
- B.Device1
- C.a Log Analytics workspace

Answer: D

Question: 183

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to configure an update ring that meets the following requirements:

- Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
- The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
- Devices must restart automatically three days after an update is installed.

How should you configure the update ring? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Feature update deferral period (days):

	▼
3	
7	
10	
14	
90	

Quality update deferral period (days):

	▼
3	
7	
10	
14	
90	

Deadline for feature updates:

	▼
3	
7	
10	
14	
90	

Grace period:

	▼
3	
7	
10	
14	
90	

Answer:

Answer Area

Feature update deferral period (days):

▼
3
7
10
14
90

Quality update deferral period (days):

▼
3
7
10
14
90

Deadline for feature updates:

▼
3
7
10
14
90

Grace period:

▼
3
7
10
14
90

Question: 184

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You need to review and implement Microsoft 365 Defender device onboarding. The solution must meet the following requirements:












- View onboarded devices that have the Chromium-based version for Microsoft Edge installed.
- Download an onboarding package for a Windows 11 device.
- Minimize administrative effort.

Which two settings should you use in the Microsoft 365 Defender portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

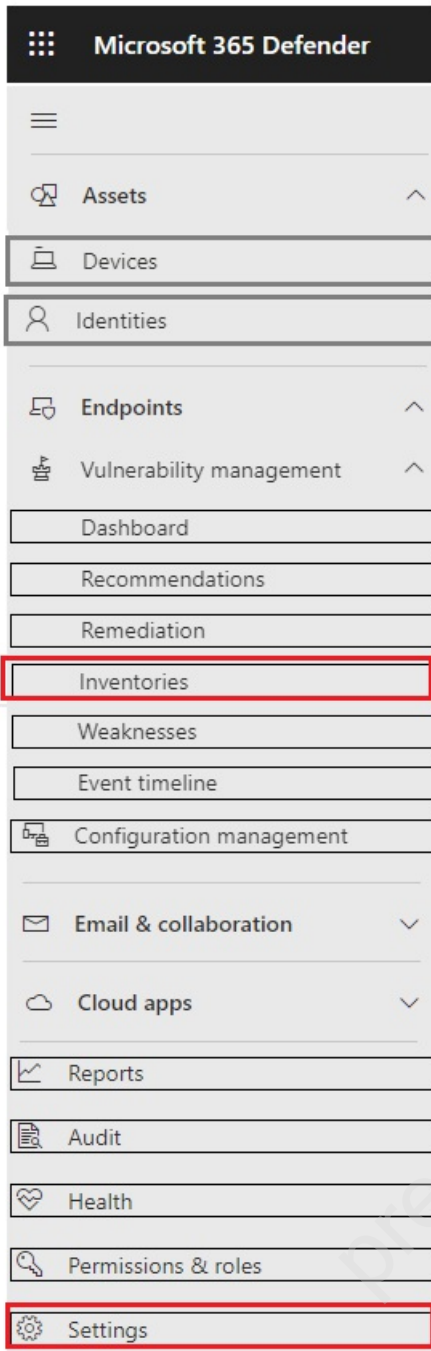
Answer Area



	Identities	
	Endpoints	^
	Vulnerability management	^
	Dashboard	
	Recommendations	
	Remediation	
	Inventories	
	Weaknesses	
	Event timeline	
	Configuration management	
	Email & collaboration	v
	Cloud apps	v
	Reports	
	Audit	
	Health	
	Permissions & roles	
	Settings	

Answer:

Answer Area



Question: 185

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender Antivirus.

What should you do?

- A. From the Microsoft Intune admin center, create a security baseline.
- B. From the Microsoft 365 Defender portal, enable tamper protection.
- C. From the Microsoft Intune admin center, create an account protection policy.
- D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Answer: B

Question: 186

HOTSPOT

-

You have 1,000 computers that run Windows 10 and are members of an Active Directory domain.

You need to capture the event logs from the computers to Azure.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure service to provision:

▼

An Azure Storage account

Azure Cosmos DB

Azure SQL Database

Log Analytics

Action to perform on the computers:

▼

Create a collector-initiated subscription

Install the Azure Monitor Agent

Enroll in Microsoft Intune

Register to Azure AD

Answer:

Answer Area

Azure service to provision:

▼

An Azure Storage account
Azure Cosmos DB
Azure SQL Database
Log Analytics

Action to perform on the computers:

▼

Create a collector-initiated subscription
Install the Azure Monitor Agent
Enroll in Microsoft Intune
Register to Azure AD

Question: 187

You have a computer named Computer5 that has Windows 10 installed.

You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5.

Which file should you modify on Computer5?

- A.LiteTouch.wsf
- B.SetupConfig.ini
- C.Unattend.bat
- D.Unattend.xml

Answer: B

Question: 188

HOTSPOT

-

You have a Microsoft 365 tenant and an internal certification authority (CA).

You need to use Microsoft Intune to deploy the root CA certificate to managed devices.

Which type of Intune policy and profile type template should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

▼

App configuration policy
App protection policy
Compliance policy
Configuration profile

Profile type template:

▼

Imported public key pair (PKCS) certificate
Public key pair (PKCS) certificate
Simple Certificate Enrollment Protocol (SCEP) certificate
Trusted certificate

Answer:

Answer Area

Policy type:

▼

App configuration policy
App protection policy
Compliance policy
Configuration profile

Profile type template:

▼

Imported public key pair (PKCS) certificate
Public key pair (PKCS) certificate
Simple Certificate Enrollment Protocol (SCEP) certificate
Trusted certificate

Question: 189

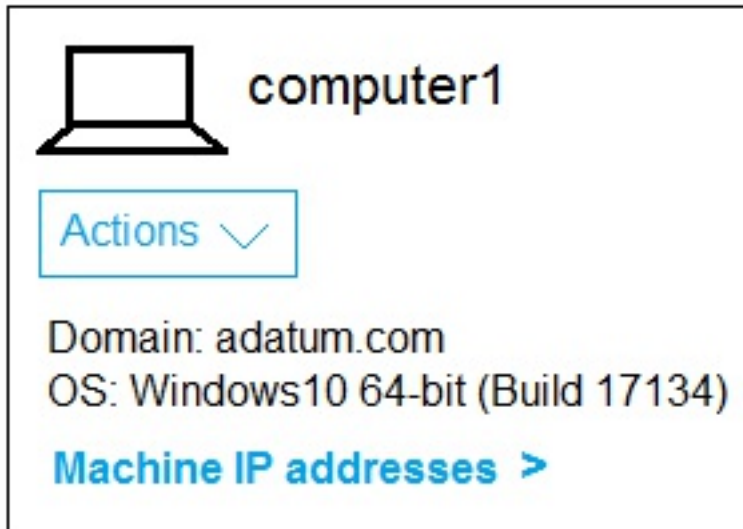
HOTSPOT

-

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped devices (default)	Not applicable

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:

▼

- Group3 only
- Group4 only
- Group5 only
- Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

▼

- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

Answer:

Answer Area

Computer1 will be a member of:

Group3 only
Group4 only
Group5 only
Group3, Group4, and Group5 only

If you add the tag demo to Computer1,
Computer1 will be a member of:

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

Question: 190

You manage 1,000 devices by using Microsoft Intune.

You review the Device compliance trends report.

For how long will the report display trend data?

- A.30 days
- B.60 days
- C.90 days
- D.365 days

Answer: B

Question: 191

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released.

What should you create?

- A.an iOS app provisioning profile
- B.a device configuration profile based on the Device features templates
- C.an update policy for iOS/iPadOS
- D.a device configuration profile based on the Device restrictions template

Answer: D

Question: 192

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices.

You need to create Intune configuration profiles to perform the following actions on the devices:

- Deploy a custom Start layout.
- Rename the local Administrator account.

Which profile type template should you use for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Deploy a custom Start layout:

	▼
Delivery optimization	
Device restriction	
Endpoint protection	
Identity protection	

Rename the local Administrator account:

	▼
Delivery optimization	
Device restriction	
Endpoint protection	
Identity protection	

Answer:

Answer Area

Deploy a custom Start layout:

▼

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

▼

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Question: 193

HOTSPOT

-

You have a Microsoft 365 subscription.

You plan to enable Microsoft Intune enrollment for the following types of devices:

- Existing Windows 11 devices managed by using Configuration Manager
- Personal iOS devices

The solution must minimize user disruption.

Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 11 devices managed by using Configuration Manager:

▼

Co-management
User enrollment
Windows Autopilot

Personal iOS devices:

▼

Apple Configurator
Automated Device Enrollment (ADE)
User enrollment

Answer:

Answer Area

Windows 11 devices managed by using Configuration Manager:

▼

Co-management
User enrollment
Windows Autopilot

Personal iOS devices:

▼

Apple Configurator
Automated Device Enrollment (ADE)
User enrollment

Question: 194

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune.

Device1 is managed by using Group Policy and Intune.

You need to ensure that the Intune settings override the Group Policy settings.

What should you configure?

- A.a device configuration profile
- B.a device compliance policy
- C.an MDM Security Baseline profile
- D.a Group Policy Object (GPO)

Answer: A

Question: 195

HOTSPOT

-

You have an Azure AD Premium P2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- MDM user scope: Group1
- MAM user scope: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment. <input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>


Question: 196


HOTSPOT


You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)

[Home](#) > [Endpoint security](#) > [MDM Security Baseline](#) >


Create profile

Block Office applications from injecting code into other processes ⓘ Disable 

Block Office applications from creating executable content ⓘ Audit mode 

Block all Office applications from creating child processes ⓘ Audit mode 

Block Win32 API calls from Office macro ⓘ Disable 

Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ Disable 

You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)

Edit Profile

^ Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe)



Audit mode



Block Adobe Reader from creating child processes



Audit mode



Block Office applications from injecting code into other processes



Audit mode



Block Office applications from creating executable content



Audit mode



Block all Office applications from creating child processes



Audit mode



Block Win32 API calls from Office macro 

Audit mode



You plan to deploy both profiles to devices enrolled in Microsoft Intune.

You need to identify how the following settings will be configured on the devices:

- Block Office applications from creating executable content
- Block Win32 API calls from Office macro

Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Block Office applications from creating executable content:

▼

Audit mode
Block
Disable
Warn

Block Win32 API calls from Office macro:

▼

Audit mode
Block
Disable
Warn

Answer:

Answer Area

Block Office applications from creating executable content:

▼

Audit mode
Block
Disable
Warn

Block Win32 API calls from Office macro:

▼

Audit mode
Block
Disable
Warn

Question: 197

DRAG DROP

-

You have an on-premises Active Directory domain that syncs to Azure AD tenant.

The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune.

The Microsoft Office settings on the computers are configured by using a Group Policy Object (GPO).

You need to migrate the GPO to Intune.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

Answer Area

1

2

3

>

<

^

v

Answer:

Answer Area

- 1 Create a configuration profile.
- 2 Configure the Administrative Templates settings.
- 3 Assign the profile.

Question: 198

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains 100 client computers that run Windows 10.

Currently, your company does NOT have a deployment infrastructure.

The company purchases Windows 11 licenses through a volume licensing agreement.

You need to recommend how to upgrade the computers to Windows 11. The solution must minimize licensing costs.

What should you include in the recommendation?

- A.Windows Autopilot
- B.Configuration Manager
- C.subscription activation
- D.Microsoft Deployment Toolkit (MDT)

Answer: D

Question: 199

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices that run Windows 11.

You need to remove User1 from the local Administrators group on all enrolled devices.

What should you configure?

- A.a device compliance policy

- B.an account protection policy
- C.an app configuration policy

Answer: B

Question: 200

HOTSPOT

-

You have computers that run Windows 10 and are configured by using Windows Autopilot.

A user performs the following tasks on a computer named Computer1:

- Creates a VPN connection to the corporate network
- Installs a Microsoft Store app named App1
- Connections to a Wi-Fi network

You perform a Windows Autopilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The Wi-Fi connection will be:

- Removed
- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:

- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Answer:

Answer Area

The Wi-Fi connection will be:

- Removed
- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:

- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Question: 201

HOTSPOT

-

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.

MDT contains the operating system images shown in the following table.

Name	Description
Image1.wim	Custom-built Windows 11 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 11 image without apps
Install.wim	Default Windows 11 image

You need to perform a Windows 11-place upgrade on several computers that run Windows 10.

From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

▼

Standard Client Task Sequence
Standard Client Replace Task Sequence
Standard Client Upgrade Task Sequence

Operating system image:

▼

Image1.wim
Image2.wim
Install.wim

Answer:

Answer Area

Task sequence template:

▼

Standard Client Task Sequence
Standard Client Replace Task Sequence
Standard Client Upgrade Task Sequence

Operating system image:

▼

Image1.wim
Image2.wim
Install.wim

Question: 202

You have a workgroup computer named Client1 that runs Windows 11 and connects to a public network.

You need to enable PowerShell remoting on Client1. The solution must ensure that PowerShell remoting connections are accepted from the local subnet only.

Which PowerShell command should you run?

- A. Set-PSSessionConfiguration -AccessMode Local
- B. Enable-PSRemoting -SkipNetworkProfileCheck
- C. Enable-PSRemoting -Force
- D. Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any

Answer: B

Question: 203

HOTSPOT

-

You have a Microsoft 365 subscription.

You need to enable passwordless authentication for all users. The solution must meet the following requirements:

- Users in the research department cannot use mobile devices and must authenticate from unmanaged Linux devices by using an alternative method.
- To access services, users in the sales department must authenticate by using their mobile phone.
- Administrative effort must be minimized.

Which authentication method should you use for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sales:

FIDO2 security keys
Microsoft Authenticator
Temporary Access Pass
Windows Hello for Business

Research:

FIDO2 security keys
Microsoft Authenticator
Temporary Access Pass
Windows Hello for Business

Answer:

Answer Area

Sales:

FIDO2 security keys
Microsoft Authenticator
Temporary Access Pass
Windows Hello for Business

Research:

FIDO2 security keys
Microsoft Authenticator
Temporary Access Pass
Windows Hello for Business

Question: 204

HOTSPOT

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft Intune.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)

Create policy

✓ Basics **2 Apps** ③ Data protection ④ Access requirements ⑤ Conditional launch ⑥ Assignments ⑦ Review + create

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types ⓘ

Yes

No

Device types * ⓘ

Unmanaged

Public apps

Remove

Microsoft Outlook

Remove

+ Select public apps

Custom apps

Remove

No custom apps selected

+ Select custom apps

Previous

Next

You need to configure the policy to meet the following requirements:

- Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.
- Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Prevent the users from using Outlook
if the operating system version is less than 12.0.0:

▼

Access requirements
Conditional launch
Data protection
Scope

Require the users to use an alphanumeric
passcode to access Outlook:

▼

Access requirements
Conditional launch
Data protection
Scope

Answer:

Answer Area

Prevent the users from using Outlook
if the operating system version is less than 12.0.0:

▼

Access requirements
Conditional launch
Data protection
Scope

Require the users to use an alphanumeric
passcode to access Outlook:

▼

Access requirements
Conditional launch
Data protection
Scope

You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune.

You need to review the servicing status of a computer.

What should you do?

- A.From Device configuration – Profiles, view the device status.
- B.From Software updates, view the Per update ring deployment state.
- C.From Software updates, view the audit logs.
- D.From Device compliance, view the device compliance.

Answer: B

Question: 206

HOTSPOT

-

Your network contains an Active Directory domain. Active Directory is synced with Azure AD.

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tool to use to configure the settings:

▼

Microsoft Purview compliance portal
Windows Security app
Microsoft Intune admin center

Distribution method:

▼

An Azure policy
An Endpoint Protection configuration profile
An Intune device compliance policy
A device restrictions configuration profile

Answer:

Answer Area

Tool to use to configure the settings:

Microsoft Purview compliance portal
Windows Security app
Microsoft Intune admin center

Distribution method:

An Azure policy
An Endpoint Protection configuration profile
An Intune device compliance policy
A device restrictions configuration profile

Question: 207

You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.

Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.

You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.

Which DNS records do you need?

- A.one TXT record only
- B.three CNAME records
- C.three TXT records
- D.one CNAME record only

Answer: B

Question: 208

HOTSPOT

-

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Intune that have the platforms and versions shown in the following table.

Platform	Version
Android	8,9
iOS	11,12

You need to configure device enrollment to meet the following requirements:

- Ensure that only devices that have approved platforms and versions can enroll in Microsoft Intune.

•Ensure that devices are added to Azure AD groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Microsoft Intune:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Answer:

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Microsoft Intune:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions**
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories**
- Enrollment restrictions
- Windows enrollment

Question: 209

HOTSPOT

-

You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device.

Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

▼

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

Device2:

▼

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

RBAC role:

▼

Help Desk Operator
Application Manager
Intune Role Administrator
Policy and Profile Manager

Answer:

Answer Area

Device1:

▼

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

Device2:

▼

FileVault
Cryptsetup
Encrypting File System (EFS)
BitLocker Drive Encryption (BitLocker)

RBAC role:

▼

Help Desk Operator
Application Manager
Intune Role Administrator
Policy and Profile Manager

Question: 210

DRAG DROP

Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Intune.

You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Create a Microsoft SharePoint Online site.

Purchase an Azure subscription.

Add diagnostic settings.

Install Microsoft Power BI Desktop.

Create a Log Analytics workspace.

Add a certificate connector to Microsoft Intune.



Answer:

Answer Area

Purchase an Azure subscription.

Create a Log Analytics workspace.

Add diagnostic settings.

Question: 211

DRAG DROP

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You plan to onboard the following types of devices to Defender for Endpoint:

- macOS
- Linux Server

What should you use to onboard each device? To answer, drag the appropriate tools to the correct device types. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Tools

Answer Area

Ansible

Group Policy

Microsoft Intune

Virtual Desktop Infrastructure (VDI) scripts

macOS:

Linux Server:

Answer:

Answer Area

macOS: Microsoft Intune

Linux Server: Ansible

Question: 212

You have a Windows 10 device named Computer1 enrolled in Microsoft Intune.

You need to configure Computer1 as a public workstation that will run a single customer-facing, full-screen application.

Which configuration profile type template should you use in Microsoft Intune admin center?

- A.Shared multi-user device
- B.Device restrictions
- C.Kiosk
- D.Endpoint protection

Answer: C

Question: 213

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage Windows 11 devices.

You create a new policy set named Set and add five device configuration profiles for Windows 10 and later.

You create a device compliance policy named Policy1.

You need to ensure that when users are assigned the device configuration profiles in Set1, they are always assigned Policy1 also.

What should you configure?

- A.the assignments of Policy1
- B.the Policy1 configurations
- C.the assignments of Set1
- D.the Set1 configurations

Answer: D

Question: 214

HOTSPOT

-

Your network contains an on-premises Active Directory domain that contains the locations shown in the following table.

Name	Internal IP address	Public Network Address Translation (NAT) IP address	Active Directory site
Location1	10.10.0.0/16	131.107.15.0/24	Site1
Location2	10.20.0.0/16	131.107.16.0/24	Site1
Location3	172.16.0.0/16	131.107.196.0/24	Site2

In Microsoft Intune, you enroll the Windows 10 devices shown in the following table.

Name	IP address
Device1	10.10.0.50
Device2	10.20.1.150
Device3	10.10.1.155
Device4	172.16.0.30

You have a Delivery Optimization device configuration profile applied to all the devices. The profile is configured as shown in the following exhibit.

Delivery Optimization

Windows 10 and later

✓ Basics **2 Configuration settings** 3 Assignments

If you already configured and deployed Delivery Optimization download mode in Windows 10 update rings, before you begin, go to Software updates – Windows 10 update rings and migrate your existing settings

[Learn more](#)

Download mode ⓘ

HTTP blended with peering across private group (2) ▼

Restrict Peer Selection ⓘ

Subnet mask ▼

Group ID source ⓘ

AD site ▼

Previous

Next

From which devices can Device1 and Device2 get updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1: ▼

Can get updates from Device3 only.
Cannot get updates from any device.
Can get updates from Device1 and Device3 only.
Can get updates from Device1, Device3, and Device4.

Device2: ▼

Can get updates from Device3 only.
Cannot get updates from any device.
Can get updates from Device1 and Device3 only.
Can get updates from Device1, Device3, and Device4.

Answer:

Answer Area

Device1: ▼

Can get updates from Device3 only.
Cannot get updates from any device.
Can get updates from Device1 and Device3 only.
Can get updates from Device1, Device3, and Device4.

Device2: ▼

Can get updates from Device3 only.
Cannot get updates from any device.
Can get updates from Device1 and Device3 only.
Can get updates from Device1, Device3, and Device4.

Question: 215

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to enable self-service password reset on the sign-in screen.

Which settings should you configure from the Microsoft Intune admin center?

- A.Device configuration
- B.Device enrollment
- C.Conditional access
- D.Device compliance

Answer: A

Question: 216

HOTSPOT

-

You have a Microsoft 365 tenant that uses Microsoft Intune.

From the Microsoft Intune admin center, you plan to create a baseline to monitor the Startup score and the App reliability score of enrolled Windows 10 devices.

You need to identify which tool to use to create the baseline and the minimum number of devices required to create the baseline.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tool to use:

▼

Workloads
Log Analytics
Endpoint analytics
Security baselines

Minimum number of devices:

▼

1
5
10
25

Answer:

Answer Area

Tool to use:

▼

Workloads

Log Analytics

Endpoint analytics

Security baselines

Minimum number of devices:

▼

1

5

10

25

Question: 217

You are implementing Microsoft Intune Suite.

You enroll devices in Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

The performance of which devices can be analyzed by using Endpoint analytics?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1, Device2, and Device3 only
- D.Device1, Device2, and Device4 only
- E.Device1, Device2, Device3, and Device4

Answer: B

Question: 218

You have the devices shown in the following table.

Name	Operating system	Domain member
Device1	Windows 11 Enterprise	No
Device2	Windows 10 Pro	Yes
Device3	Android	No
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.

What should you identify?

- A.Device1 only
- B.Device2 only
- C.Device1, Device2 only
- D.Device1, Device2, and Device3 only
- E.Device1, Device2, Device3, and Device4

Answer: D

Question: 219

You have a Microsoft 365 subscription.

You use app protection policies to protect corporate data on Android devices.

You need to ensure that any user connecting from an Android device can only access the corporate data if they connect from an app that supports mobile application management (MAM).

What should you configure?

- A.an app configuration policy
- B.a Conditional Access policy
- C.a device configuration profile
- D.a device compliance policy

Answer: B

Question: 220

Your company has a Microsoft 365 subscription.

All the users in the finance department own personal devices that run iOS or Android. All the devices are enrolled in Microsoft Intune.

The finance department adds new users each month.

The company develops a mobile application named App1 for the finance department users.

You need to ensure that only the finance department users can download App1.

What should you do first?

- A.Register App1 in Azure AD.
- B.Add App1 to the vendor stores for iOS and Android applications.
- C.Add App1 to a Microsoft Deployment Toolkit (MDT) deployment share.
- D.Add App1 to Intune.

Answer: D

Question: 221

DRAG DROP

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform	Enrolled in Microsoft Intune
Device1	Windows 10	Yes
Device2	Android Enterprise	Yes
Device3	iOS/iPadOS	Yes

You need to configure the Microsoft Edge settings for each device.

What should you use? To answer, drag the appropriate Intune features to the correct devices. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Intune Features

Answer Area

App configuration policy

Device compliance policy

Device configuration profile

Endpoint security policy

Device1:

Device2:

Device3:

Answer:

Answer Area

Device1: Device configuration profile

Device2: App configuration policy

Device3: App configuration policy

Question: 222

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1.

All the users use Microsoft Excel.

From the Microsoft Intune admin center, you create the policies shown in the following table.

Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet(*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook(*.xlsb)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	<input type="radio"/>	<input type="radio"/>
When User2 saves a new spreadsheet, the .xlsb format is used.	<input type="radio"/>	<input type="radio"/>
When User3 saves a new spreadsheet, the .xlsx format is used.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 saves a new spreadsheet, the .xlsb format is used.	<input type="radio"/>	<input checked="" type="radio"/>
When User3 saves a new spreadsheet, the .xlsx format is used.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 223

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains a computer named Computer1 that runs Windows 11. Computer1 is enrolled in Microsoft Intune.

You need to deploy an app named App1 to Computer1. The App1 installation will use multiple files.

What should you use to package App1, and which file format will be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use:

Deployment Image Servicing and Management (DISM)
Microsoft Application Virtualization (App-V) Sequencer
Win32 Content Prep Tool
Windows Package Manager

File format:

.apk
.appv
.intunewin
.ipa

Answer:

Answer Area

Use:

Deployment Image Servicing and Management (DISM)
Microsoft Application Virtualization (App-V) Sequencer
Win32 Content Prep Tool
Windows Package Manager

File format:

.apk
.appv
.intunewin
.ipa

Question: 224

You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do from the Microsoft Intune admin center?

- A.From Device compliance, configure the Compliance policy settings.
- B.From Endpoint security, configure the Conditional access settings.
- C.From Tenant administration, modify the Diagnostic settings.
- D.From Policy1, modify the actions for noncompliance.

Answer: A

Question: 225

HOTSPOT

-

Your company has an infrastructure that has the following:

- A Microsoft 365 tenant
- An Active Directory forest
- Microsoft Intune
- A Key Management Service (KMS) server
- A Windows Deployment Services (WDS) server
- An Azure AD Premium tenant

The company purchases 100 new client computers that run Windows.

You need to ensure that the new computers are joined automatically to Azure AD by using Windows Autopilot.

What should you use? To answer, select the appropriate options in the answer area,

NOTE: Each correct selection is worth one point.

Answer Area

Management tool:

Microsoft Entra admin center
Microsoft Intune admin center
Volume Activation Management Tool console
Windows Deployment Services console

Required information
from each computer:

Device serial number and hardware hash
MAC address and computer name
Volume License Key and computer name

Answer:

Answer Area

Management tool:

Microsoft Entra admin center
Microsoft Intune admin center
Volume Activation Management Tool console
Windows Deployment Services console

Required information
from each computer:

Device serial number and hardware hash
MAC address and computer name
Volume License Key and computer name

Question: 226

You have an Azure AD tenant named contoso.com.

You plan to purchase 25 computers that run Windows 11. You plan to deliver the computers directly to users.

You need to ensure that during the out-of-box experience (OBE), users are prompted to sign in, and then the computers are configured to use Microsoft Intune.

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.a provisioning package
- B.automatic enrollment
- C.an unattend.xml answer file
- D.a Windows Autopilot deployment profile for self-deploying mode
- E.a Windows Autopilot deployment profile for user-driven mode

Answer: BE

Question: 227

You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.Create an Azure AD group that has dynamic membership rules and uses the ZTDID tag.
- B.Create an Azure AD group that has dynamic membership rules and uses the operatingSystem tag.
- C.Assign a Windows Autopilot deployment profile to a group.
- D.Join the computers to Azure AD.
- E.Create a Group Policy object (GPO) that is linked to a domain.
- F.Join the computers to an on-premises Active Directory domain.

Answer: AC

Question: 228

DRAG DROP

-

You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare.

You need to add a feature pack to the boot image.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

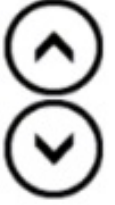
Copy the feature pack
to D:\MDTShare\Tools\x86.

Copy the feature pack
to D:\MDTShare\Packages.

Modify the Windows PE properties
of the deployment share.

Modify the General properties
of the deployment share.

Update the deployment share.



Answer:

Answer Area

Copy the feature pack
to D:\MDTShare\Tools\x86.

Modify the Windows PE properties
of the deployment share.

Update the deployment share.

Question: 229

You plan to deploy Windows 11 Pro to 200 new computers by using the Microsoft Deployment Toolkit (MDT) and Windows Deployment Services (WDS).

The company has a Volume Licensing Agreement and uses a product key to activate Windows 11.

You need to ensure that the new computers will be configured to have the correct product key during the installation.

What should you configure?

- A. an MDT task sequence
- B. the Device settings in Azure AD
- C. a WDS boot image

Answer: A

Question: 230

HOTSPOT

-

You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of-Box Drivers folder named Windows 11 x64 that has subfolders in the format of make name \ model name .

You need to modify a deployment task sequence to ensure that all the drivers in the folder that match the make and model of the computers are installed without using PnP detection or selection profiles.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Phase that you must modify
in the deployment task sequence:

▼

Install
Preinstall
Validation

Task that you must use to specify
which folder contains the drivers:

▼

Gather
Inject Drivers
Set Task Sequence Variable
Validate

Answer:

Answer Area

Phase that you must modify
in the deployment task sequence:

	▼
Install	
Preinstall	
Validation	

Task that you must use to specify
which folder contains the drivers:

	▼
Gather	
Inject Drivers	
Set Task Sequence Variable	
Validate	

Question: 231

HOTSPOT

-

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.

You need to modify the deployment share to meet the following requirements:

- Ensure that the user who performs the installation is prompted to set the local Administrator password
- Define a rule for how to name computers during the deployment.

The solution must NOT replace the existing WinPE image.

Which file should you modify for each requirement? To answer, select the appropriate options in the answer area,

NOTE: Each correct selection is worth one point.

Answer Area

Administrator password:

▼

Bootstrap.ini
CustomSettings.ini
Settings.ini
System.ini

Computer names:

▼

Bootstrap.ini
CustomSettings.ini
Settings.ini
System.ini

Answer:

Answer Area

Administrator password:

▼

Bootstrap.ini
CustomSettings.ini
Settings.ini
System.ini

Computer names:

▼

Bootstrap.ini
CustomSettings.ini
Settings.ini
System.ini

Question: 232

HOTSPOT

-

You have an Azure AD tenant that contains the following:

- Windows 11 devices that are joined to Azure AD
- A user that has a display name of User1 and a UPN of

You enable Remote Desktop on the Windows 11 devices.

You need to ensure that User1 can use Remote Desktop to connect to the devices.

How should you complete the command that must be run on each device? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

net localgroup /add

Answer:

Answer Area

net localgroup /add

Question: 233

HOTSPOT

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	RAM	Storage	TPM version
Device1	14 GB	256 GB	1.2
Device2	4 GB	64 GB	2.0
Device3	8 GB	128 GB	2.0

All the devices will be reimaged and licensed by using subscription activation.

The devices are assigned to the users shown in the following table.

Name	Device	License
User1	Device1	Microsoft 365 E5
User2	Device2	Microsoft 365 E3
User3	Device3	Office 365 E5, Enterprise Mobility + Security E5

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 can be upgraded to Windows 11 and activated.	<input type="radio"/>	<input type="radio"/>
Device2 requires additional hardware before it can be upgraded to Windows 11.	<input type="radio"/>	<input type="radio"/>
User3 requires an additional license to activate Windows 11 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 can be upgraded to Windows 11 and activated.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 requires additional hardware before it can be upgraded to Windows 11.	<input type="radio"/>	<input checked="" type="radio"/>
User3 requires an additional license to activate Windows 11 on Device3.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 234

Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 10. Users in the finance department use the computers.

You have a computer named Computer1 that runs Windows 10.

From Computer1, you plan to run a script that executes Windows PowerShell commands on the finance department computers.

You need to ensure that you can run the PowerShell commands on the finance department computers from Computer.

What should you do on the finance department computers?

- A.From Windows PowerShell, run the Enable-MMAgent cmdlet.
- B.From the local Group Policy, enable the Allow Remote Shell Access setting.

- C.From Windows PowerShell, run the Enable-PSRemoting cmdlet.
- D.From the local Group Policy, enable the Turn on Script Execution setting.

Answer: C

Question: 235

You have a Microsoft 365 subscription that includes Microsoft Intune.

You plan to use Windows Autopilot to deploy Windows 11 devices.

You need to meet the following requirements during Autopilot provisioning:

- Display the app and profile configuration progress.
- Block users from using the devices until all apps and profiles are installed

What should you configure?

- A.an app configuration policy
- B.an app protection policy
- C.an enrollment device platform restriction
- D.an enrollment status page

Answer: D

Question: 236

HOTSPOT

-

You have a Microsoft 365 subscription. The subscription contains 1,000 computers that run Windows 11 and are enrolled in Microsoft Intune.

You plan to create a compliance policy that has the following options enabled:

- Require Secure Boot to be enabled on the device.
- Require the device to be at or under the machine risk score.

Which two Compliance settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10/11 compliance policy ...

Windows 10 and later

- ✓ Basics ② Compliance settings ③ Actions for noncompliance ④ Assignments ⑤ Review + create

▼ Custom Compliance
▼ Device Health
▼ Device Properties
▼ Configuration Manager Compliance
▼ System Security
▼ Microsoft Defender for Endpoint

Answer:

Answer Area

Windows 10/11 compliance policy ...

Windows 10 and later

- ✓ Basics ② Compliance settings ③ Actions for noncompliance ④ Assignments ⑤ Review + create

▼ Custom Compliance
▼ Device Health
▼ Device Properties
▼ Configuration Manager Compliance
▼ System Security
▼ Microsoft Defender for Endpoint

Question: 237

Your network contains an Active Directory domain named contoso.com. The domain contains 25 computers that run Windows 11.

You have a Microsoft 365 subscription

You have an Azure AD tenant that syncs with contoso.com.

You configure hybrid Azure AD join and discover that some of the computers have a registered state of Pending.

You need to ensure that the computers complete the join successfully.

What should you ensure?

- A.that Windows is activated on all the computers
- B.that the users of the computers are assigned Microsoft 365 licenses
- C.that each computer has a line of sight to a domain controller
- D.that the computers contain the latest quality updates

Answer: C

Question: 238

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows
Device2	Android
Device3	iOS
Device4	macOS

For which devices can you manage updates by using Intune?

- A.Device1 only
- B. Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device3, and Device4 only
- E.Device1, Device2, Device3, and Device4

Answer: E

Question: 239

You have 500 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You plan to distribute certificates to the computers by using Simple Certificate Enrollment Protocol (SCEP).

You have the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Root certification authority (CA)
Server3	Subordinate certification authority (CA)
Server4	Network Device Enrollment Service (NDES)

NDES issues certificates from the subordinate CA.

You are configuring a device configuration profile as shown in the exhibit. (Click the Exhibit tab.)

SCEP certificate

Windows 10 and later

- ✓ Basics
- ✓ Configuration settings
- ✓ Assignments
- ✓ Applicability Rules
- 5 Review + create

Certificate type

User

Subject name format * ⓘ

Common name including email

Subject alternative name ⓘ

2 selected

Certificate validity period * ⓘ

Years

1

Key storage provider (KSP) * ⓘ

Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP

Key usage * ⓘ

2 selected

Key size (bits) * ⓘ

2048

Hash algorithm * ⓘ

SHA-2

Root Certificate * ⓘ

+ Root Certificate

Extended key usage * ⓘ

Export

Name	Object Identifier	Predefined values
Not configured	Not configured	Not configured

You need to complete the SCEP profile.

On which server is the required root certificate located?

- A.Server1
- B.Server2
- C.Server3
- D.Server4

Answer: C

Question: 240

HOTSPOT

-

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.

How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Answer:

Answer Area

Device1:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Question: 241

HOTSPOT

You have two Windows 10 devices enrolled in Microsoft Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Enabled	Group2
Device2	Disabled	Group1


The Compliance policy settings are configured as shown in the following exhibit.



Compliance policy settings

 Save  Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as  Compliant Not Compliant

Enhanced jailbreak detection  Enabled Disabled

Compliance status validity period (days)  

On August 1, you create a compliance policy as shown in the following exhibit.

Windows 10 compliance policy

Windows 10 and later

 Basics  Compliance settings  Actions for noncompliance  Assignments 5 Review + create

Summary

Basics

Name Compliance1
Description --
Platform Windows 10 and later
Profile type Windows 10 compliance policy

Compliance settings

Require BitLocker Require

Actions for noncompliance

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	3 days		
Retire the noncompliant device	5 days		

Assignments

Included groups Group1
Excluded groups Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is marked as compliant on August 4.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant on August 2.	<input type="radio"/>	<input type="radio"/>
Device2 is retired on August 6.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant on August 4.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is marked as compliant on August 2.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is retired on August 6.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 242

HOTSPOT

-

You have 100 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune.

You need to configure the following device restrictions:

- Block users from browsing to suspicious websites.
- Scan all scripts loaded into Microsoft Edge.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device restrictions

Windows 10 and later

- ✓ Microsoft Edge Browser
- ✓ Network proxy
- ✓ Password
- ✓ Per-app privacy exceptions
- ✓ Personalization
- ✓ Printer
- ✓ Privacy
- ✓ Projection
- ✓ Reporting and Telemetry
- ✓ Search
- ✓ Start
- ✓ Microsoft Defender SmartScreen
- ✓ Windows Spotlight
- ✓ Microsoft Defender Antivirus

Previous

Next

Answer:

Answer Area

Device restrictions

Windows 10 and later

- ✓ Microsoft Edge Browser
- ✓ Network proxy
- ✓ Password
- ✓ Per-app privacy exceptions
- ✓ Personalization
- ✓ Printer
- ✓ Privacy
- ✓ Projection
- ✓ Reporting and Telemetry
- ✓ Search
- ✓ Start
- ✓ Microsoft Defender SmartScreen
- ✓ Windows Spotlight
- ✓ Microsoft Defender Antivirus

Previous

Next

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Description
Device1	User-enrolled Windows 11 device
Device2	Auto-enrolled Windows 10 device
Device3	User-enrolled Android device
Device4	User-enrolled iOS device

You need to identify the following:

- Device you can remove from Intune by using the Wipe action.
- The enrollment state and the associated user account can be retained on devices that are wiped.

What should you identify? To answer, select the appropriate options in the answer area.

Answer Area

Devices you can remove from Intune by using the Wipe action:

▼

Device1 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, and Device4 only
Device1, Device2, Device3, and Device4

The enrollment state and the associated user account can be retained on devices that are wiped:

▼

Device1 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, and Device4 only
Device1, Device2, Device3, and Device4

Answer:

Answer Area

Devices you can remove from Intune by using the Wipe action:

▼

Device1 only

Device1 and Device2 only

Device1, Device2, and Device3 only

Device1, Device2, and Device4 only

Device1, Device2, Device3, and Device4

The enrollment state and the associated user account can be retained on devices that are wiped:

▼

Device1 only

Device1 and Device2 only

Device1, Device2, and Device3 only

Device1, Device2, and Device4 only

Device1, Device2, Device3, and Device4

Question: 244

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes





The tenant contains the Azure AD groups shown in the following table.

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

You add an Autopilot deployment profile as shown in the following exhibit.

Create profile ...

Windows PC

-  Basics  Out-of-box experience (OOBE)  Assignments  **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 245

HOTSPOT

-

You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production.

You configure the following settings in the Bootstrap.ini file.

[Settings]

Priority=DefaultGateway, Default

[DefaultGateway]

10.1.1.1=NewYork

10.5.5.1=London

[NewYork]

DeployRoot=\\MDT1\Production\$

[London]

DeployRoot=\\MDT2\Production\$

KeyboardLocale=en-gb

[Default]

DeployRoot=\\MDT3\Production\$

KeyboardLocale=en-us

You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
TB1 will download the image from MDT3.	<input type="radio"/>	<input type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

Yes

No

TB1 will download the image from MDT3. ☐

☒

DT1 will have a KeyboardLocale of en-gb. ☒

☐

LT1 will download the image from MDT1. ☒

☐

Question: 246

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune.

You create an app configuration policy that contains the following settings:

- Device enrollment type: Managed devices
- Profile Type: All Profile Types
- Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A.Android Enterprise system app
- B.Web link
- C.Android store app
- D.Managed Google Play store app
- E.Built-in Android app

Answer: AD

Question: 247

You have a Microsoft 365 subscription.

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android
Device3	iOS
Device4	Ubuntu Linux

To which devices can you deploy apps by using Intune?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device2, and Device3 only
- E.Device1, Device2, Device3, and Device4

Answer: D

Question: 248

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You deploy Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

Name	Shows in Company Portal	Microsoft Office app to install	Assignment	Time of creation
App1	Yes	Word	Group1 – Required	10:00 AM
App2	Yes	Excel	Group2 – Required	10:30 AM
App3	Yes	PowerPoint	Group1 – Available	11:00 AM

The next day you review the results of the app deployments.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
App1 shows in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Word is installed on Device1.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
App1 shows in the Company Portal.	<input checked="" type="radio"/>	<input type="radio"/>
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 249

HOTSPOT

-

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Intune to manage devices.

You need to assess device performance during startup and identify any device models that take longer than average to start.

What should you use to assess the device performance, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use:

▼

Compliance policies
Device diagnostics
Endpoint analytics

In portal:

▼

Microsoft 365 Apps admin center
Microsoft Entra admin center
Microsoft Intune admin center

Answer:

Answer Area

Use: ▼

- Compliance policies
- Device diagnostics
- Endpoint analytics**

In portal: ▼

- Microsoft 365 Apps admin center
- Microsoft Entra admin center
- Microsoft Intune admin center**

Question: 250

DRAG DROP

-

Your on-premises network contains an Active Directory Domain Services (AD DS) domain.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains five virtual machines and is NOT connected to the on-premises network.

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You purchase Windows 365 Enterprise licenses.

You need to deploy Cloud PC. The solution must meet the following requirements:

- All users must be able to access their Cloud PC at any time without any restrictions.
- The users must be able to connect to the virtual machines on VNet1.

How should you configure the provisioning policy for Windows 365? To answer, drag the appropriate options to the correct settings. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Options

Azure network connection

Enterprise

Frontline

Microsoft Entra Hybrid Join

Microsoft Entra Join

Microsoft hosted network

Answer Area

Join type:

Network:

License type:

Answer:

Answer Area

Join type: Microsoft Entra Hybrid Join

Network: Azure network connection

License type: Enterprise

Question: 251

HOTSPOT

-

Your network contains an Active Directory domain.

The domain contains four computers named Computer1, Computer2, Computer3, and Computer4 that run Windows 10.

You perform the following actions:

- On Computer1, you install Windows Admin Center and configure Windows Defender Firewall to allow incoming communication over TCP ports 80,443, and 6516.
- On Computer2, you run the Enable-PSRemoting cmdlet.
- On Computer3, you configure Windows Defender Firewall to allow Windows Remote Management (WinRM) traffic.
- On Computer4, you run the winrm quickconfig command.

You need to manage the computers remotely by using Windows Admin Center.

From which computers can you connect to Windows Admin Center, and which computers can you manage by using Windows Admin Center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Connect from:

▼

Computer1 only
Computer1 and Computer2 only
Computer1 and Computer3 only
Computer1, Computer2, Computer3, and Computer4

Manage:

▼

Computer1 only
Computer1 and Computer2 only
Computer1 and Computer3 only
Computer1, Computer2, and Computer4 only
Computer1, Computer2, Computer3, and Computer4

Answer:

Answer Area

Connect from:

▼

Computer1 only
Computer1 and Computer2 only
Computer1 and Computer3 only
Computer1, Computer2, Computer3, and Computer4

Manage:

▼

Computer1 only
Computer1 and Computer2 only
Computer1 and Computer3 only
Computer1, Computer2, and Computer4 only
Computer1, Computer2, Computer3, and Computer4

Question: 252

You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

- A.VM1 only
- B.VM2 only
- C.VM2 and VM3 only
- D.VM1, VM2, and VM3

Answer: B

Question: 253

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Intune to manage all device.

Users have iOS devices with Microsoft apps installed.

You need to prevent users from cutting, copying, and pasting data between Microsoft Excel and other apps installed on the devices.

What should you configure?

- A.an app protection policy
- B.an app configuration policy
- C.an iOS app provisioning profile
- D.policies for Microsoft Office apps

Answer: A

Question: 254

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Intune to manage devices.

You need to review details about device wipes initiated through Intune.

Which report should you review?

- A.Noncompliant devices
- B.Assignment status

C.Windows health attestation report

D.Device actions

Answer: D

Question: 255

You have a Microsoft 365 subscription. The subscription contains 500 computers that run Windows 11 and are enrolled in Microsoft Intune.

You need to manage the deployment of monthly security updates. The solution must meet the following requirements:

- Updates must be deployed to a group of test computers for quality assurance.
- Updates must be deployed automatically 15 days after the quality assurance testing.

What should you create in the Microsoft Intune admin center?

A.a device configuration profile

B.a feature update policy

C.a security baseline

D.an update ring

Answer: D

Question: 256

HOTSPOT

-

Your company has computers that run Windows 10 and are Microsoft Entra joined.

The company purchases an Azure subscription.

You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

Answer Area

Resource to create in Azure:

An Azure event hub
An Azure Log Analytics workspace
An Azure SQL database
An Azure Storage account

Configuration to perform on the computers:

Configure the Event Collector service
Create an event subscription
Install the Azure Monitor Agent

Answer:

Answer Area

Resource to create in Azure:

An Azure event hub
An Azure Log Analytics workspace
An Azure SQL database
An Azure Storage account

Configuration to perform on the computers:

Configure the Event Collector service
Create an event subscription
Install the Azure Monitor Agent

Question: 257

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender for Endpoint.

What should you do?

- A.From the Microsoft Intune admin center, create an attack surface reduction (ASR) policy.
- B.From the Microsoft 365 Defender portal, enable tamper protection.
- C.From the Microsoft Intune admin center, create an account protection policy.
- D.From the Microsoft Entra admin center, create a Conditional Access policy.

Answer: B

Question: 258

You have a Microsoft 365 subscription that has Windows 365 Enterprise licenses.

You plan to use a custom Windows 11 image as a template for Cloud PCs.

You have a Hyper-V virtual machine that runs Windows 11 and has the following configurations:

- Name: VM1
- Disk size: 64 GB
- Disk format: VHDX
- Disk type: Fixed size
- Generation: Generation 2

You need to ensure that you can use VM1 as a source for the custom image.

What should you do on VM1 first?

- A.Change the disk type to Dynamically expanding.
- B.Change the disk format to the VHD.
- C.Change the generation to Generation 1.
- D.Increase the disk size.

Answer: B

Question: 259

HOTSPOT

-

Your on-premises network contains an Active Directory domain named contoso.com. The domain contains a user account named Admin1 and the resources shown in the following table.

Name	Type
Server1	Computer object
OU1	Organizational unit (OU)

You have a Microsoft 365 E5 subscription.

You have a Microsoft Entra tenant that syncs with contoso.com.

Admin1 plans to use Windows Autopilot to deploy 100 Windows 11 devices. The deployment must meet the following requirements:

- The devices must be Microsoft Entra hybrid joined during the deployment.
- Computer objects must be created in OU1.

You need to configure Server1 and Active Directory delegation to support the deployment.

NOTE: Each correct selection is worth one point.

Answer Area

Server1:

Enroll in Microsoft Intune.
Export the hardware hash and upload the hash to Microsoft Intune.
Install the Intune Connector for Active Directory.

Resource:

Admin1
OU1
Server1

Answer:

Answer Area

Server1:

Enroll in Microsoft Intune.
Export the hardware hash and upload the hash to Microsoft Intune.
Install the Intune Connector for Active Directory.

Resource:

Admin1
OU1
Server1

Question: 260

You have a Microsoft 365 subscription.

Each user is assigned a Windows 365 Enterprise license.

You need to deploy Cloud PCs that will be Microsoft Entra hybrid joined.

What should you do first?

- A.Create an Azure network connection (ANC).
- B.Create a provisioning policy.
- C.Create a configuration profile in Microsoft Intune.
- D.Upload a custom image.

Answer: A

Question: 261

Your on-premises network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

The domain contains a domain controller named dc1.contoso.com.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune Suite.

You have an Azure subscription that contains the resources shown in the following table.

Name	Description
LNG1	Local network gateway that uses the public IP address of the local infrastructure
GW1	Virtual network gateway
GW2	Virtual network gateway
CN1	Site-to-Site (S2S) VPN connection that connects LNG1 and GW1

The subscription contains the virtual networks shown in the following table.

Name	IP address space	Subnet	DNS configuration	Virtual network gateway
VNet1	192.168.10.0/24	192.168.10.0/26	dc1.contoso.com	GW1
VNet2	192.168.11.0/24	192.168.11.0/26	Azure DNS	None
VNet3	192.168.12.0/24	192.168.12.0/26	Azure DNS	GW2

You plan to deploy Windows 365 Enterprise Cloud PC.

You need to create an Azure network connection (ANC) that will use Microsoft Entra hybrid join.

Which virtual network can you use for the ANC?

- A.VNet1 only
- B.VNet2 only
- C.VNet3 only
- D.VNet1 and VNet2
- E.VNet1 and VNet3

Answer: A

Question: 262

DRAG DROP

-

You have a Microsoft 365 E5 subscription that includes Microsoft Intune.

The subscription contains Android Enterprise devices that are enrolled in Intune and have personally-owned work profiles. All the Android devices are members of a group named Group1.

You need to ensure that end users and Intune administrators receive an email message when an Android device does NOT have an up-to-date security provider.

Which actions should you perform from the Microsoft Intune admin center in sequence? To answer, drag the appropriate actions to the correct order. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Actions

- Create a compliance policy.
- Create a Conditional Access policy.
- Create an attack surface reduction (ASR) policy.
- From Compliance policies, create a notification message template.
- From Tenant admin, create a custom notification.

Answer Area

- Step 1:
- Step 2:
- Step 3: Assign policy to Group1.

Answer:**Answer Area**

- Step 1:
- Step 2:
- Step 3: Assign policy to Group1.

Question: 263**HOTSPOT**

You have a Microsoft 365 subscription.

You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Intune.

You need to configure the devices to meet the following requirements:

- Enable Windows Hello for Business.
- Configure Microsoft Defender SmartScreen to block users from running unverified files.

Which profile type template should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

- Windows Hello for Business:
- Microsoft Defender SmartScreen:

Answer:

Answer Area

Windows Hello for Business:

Device restrictions
Device restrictions (Windows 10 Team)
Endpoint protection
Identity protection
Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Microsoft Defender SmartScreen:

Windows health monitoring
Device restrictions (Windows 10 Team)
Endpoint protection
Identity protection
Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Question: 264

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the security groups shown in the following table.

Name	Membership type	Membership rule
Group1	Assigned	<i>Not applicable</i>
Group2	Dynamic	(device.deviceOSType -eq "Windows")
Group3	Dynamic	(extensionAttribute1 -eq "Test")

The subscription contains devices that run Windows 11, version 21H2 as shown in the following table.

Name	extensionAttribute1	Member of Group1
Device1	Test	No
Device2	<i>None</i>	No
Device3	<i>None</i>	Yes

You have a feature update deployment profile named Deployment1 as shown in the following table.

Setting	Value
Feature update to deploy	Windows 11, version 22H2
Rollout options	Make update available as soon as possible
Included groups	Group2
Excluded groups	Group1, Group3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 will be upgraded to Windows 11, version 22H2.	<input type="radio"/>	<input type="radio"/>
Device2 will be upgraded to Windows 11, version 22H2.	<input type="radio"/>	<input type="radio"/>
Device3 will be upgraded to Windows 11, version 22H2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 will be upgraded to Windows 11, version 22H2.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 will be upgraded to Windows 11, version 22H2.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 will be upgraded to Windows 11, version 22H2.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 265

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to ensure that users can only enroll devices that meet the following requirements:

- Android devices that support the use of work profiles.
- iOS devices that run iOS 11.0 or later.

Which two restrictions should you modify? To answer, select the restrictions in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

[Home](#) > [Devices](#) > [Enroll devices](#) > [All Users](#) >

Edit restriction

Device type restriction

- 1 Platform settings 2 Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more.](#)

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
Android device administrator	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
iOS/iPadOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
macOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
Windows (MDM) ①	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported

[Review + save](#)

[Cancel](#)

Answer:

Answer Area

[Home](#) > [Devices](#) > [Enroll devices](#) > [All Users](#) >

Edit restriction

Device type restriction

- 1 Platform settings 2 Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more.](#)

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
Android device administrator	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	<input type="text" value="Manufacturer name here"/>
iOS/iPadOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
macOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported
Windows (MDM) ①	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported

[Review + save](#)

[Cancel](#)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Intune to manage Windows 11 devices.

You need to implement Windows Local Administrator Password Solution (Windows LAPS).

What should you configure?

- A.a configuration profile
- B.an account protection policy
- C.an app protection policy
- D.a device compliance policy

Answer: B

Question: 267

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Microsoft Entra joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender for Endpoint on the computers.

You need to prevent users from disabling Microsoft Defender for Endpoint.

What should you do?

- A.From the Microsoft Intune admin center, create a security baseline.
- B.From the Microsoft Intune admin center, create an antivirus policy.
- C.From the Microsoft Entra admin center, create a Conditional Access policy.
- D.From the Microsoft Intune admin center, create a device compliance policy.

Answer: B

Question: 268

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to deploy a custom app to Android devices. The app uses the APK file format.

Which type of app should you select for the deployment?

- A.built-in
- B.Android store
- C.Managed Google Play
- D.line-of-business (LOB)
- E.web link

Answer: D

Question: 269

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage all devices.

You need to prepare a Win32 app named App1.exe for deployment.

What should you do first?

- A.From the Microsoft Intune admin center, create an app configuration policy.
- B.Change App1.exe to the INTUNEWIN format.
- C.From the Microsoft 365 Apps admin center, create a deployment configuration.
- D.Upload App1.exe to Azure Blob Storage.

Answer: B

Question: 270

You have a Microsoft 365 E5 subscription that includes Microsoft Intune.

For macOS devices, you create an update policy named Policy1 that has the following settings:

- All other updates (OS, built-in apps): Download and install
- Assignments:
- Included groups: All Devices

Which two types of updates can be downloaded and installed by using Policy1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.configuration file
- B.macOS
- C.firmware
- D.critical
- E.built-in app

Answer: BE

Question: 271

HOTSPOT

-

You have a Microsoft 365 E5 subscription that includes Microsoft Intune. The subscription contains a group named Group1. Group1 contains devices enrolled in Intune.

You deploy Remote Help in Intune.

You need to configure Remote Help to only allow support administrators to join Remote Help sessions from the devices in Group1.

Which type of Microsoft Entra object should you create, and which type of policy should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra object:

▼

A service principal
An app registration
An enterprise application

Policy:

▼

Compliance
Conditional Access
Endpoint Privilege Management

Answer:

Answer Area

Microsoft Entra object:

▼

A service principal
An app registration
An enterprise application

Policy:

▼

Compliance
Conditional Access
Endpoint Privilege Management

Question: 272

You have a Microsoft 365 E5 subscription that includes Microsoft Intune and contains a user named Admin1.

Admin1 must use the Microsoft Intune admin center to perform the following tasks:

- Create and assign apps and policies to users and devices by using Intune.
- Create, assign, and delete Windows 365 Cloud PC provisioning policies.

You need to assign the required roles to Admin1. The solution must meet the following requirements:

- Follow the principle of least privilege.
- Minimize administrative effort.

What should you do?

- A.Assign Admin1 the Help Desk Operator role.
- B.Assign Admin1 the Cloud PC Reader role.
- C.Assign Admin1 the Cloud PC Administrator role.
- D.Create a custom Microsoft Entra role and assign the role to Admin1.

E.Create a custom Intune role and assign the role to Admin1.

Answer: E

Question: 273

You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains Windows 11 devices enrolled in Intune. The subscription contains three groups named Department1, Department2, and Department3.

You need to deploy Microsoft 365 Apps to the Windows 11 devices. The solution must meet the following requirements:

- Users in Department1 and Department2 must receive the full Microsoft 365 Apps suite, including Microsoft Project and Visio.
- Users in Department3 must receive the full Microsoft 365 Apps suite, including Microsoft Project, but without Visio.
- All other users must receive the full Microsoft 365 Apps suite without Microsoft Project or Visio.

What is the minimum number of deployments you should create?

- A.1
- B.2
- C.3
- D.4

Answer: C

Question: 274

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You configure Intune to send log data to Log Analytics.

You need to review events involving devices that fail to enroll in Intune.

What should you monitor?

- A.operational logs
- B.audit logs
- C.the Intune Device log
- D.device compliance organizational logs

Answer: A

Question: 275

You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains corporate-owned, fully managed Android Enterprise devices.

You plan to deploy a configuration profile that will have a device restrictions profile type named Profile1. Profile1 will assign maintenance windows for system updates.

What should you configure from the Configuration settings for Profile1?

- A.Device experience
- B.General
- C.Connectivity
- D.Power Settings

Answer: B

Question: 276

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage Windows 365 Cloud PC devices.

You need to deploy a Windows 365 Security Baseline to the Cloud PC devices. The solution must meet the following requirements:

- Block data execution prevention.
- Enable virtualization-based security (VBS) and Secure Boot.

What should you configure for the Windows 365 Security Baseline profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To block data execution prevention:

	▼
File Explorer	
Microsoft Defender	
Microsoft Edge	

To enable VBS:

	▼
Device Guard	
Microsoft Defender	
System	

Answer:

Answer Area

To block data execution prevention:

▼

File Explorer

Microsoft Defender

Microsoft Edge

To enable VBS:

▼

Device Guard

Microsoft Defender

System

Question: 277

You have a Microsoft 365 subscription that includes Microsoft Intune.

You create a new Android app protection policy named Policy1 that prevents screen captures in all Microsoft apps.

You discover that an unmanaged email client installed on Android devices can still capture screens.

You need to ensure that users can only use Microsoft apps to access email.

What should you do?

- A. Create a Conditional Access policy.
- B. Create a compliance policy.
- C. Modify the Data protection settings of Policy1.
- D. Modify the assignments of Policy1.

Answer: A

Question: 278

You have a Microsoft 365 E5 subscription.

All Windows devices are enrolled in Microsoft Intune.

You need to create an app protection policy named Policy1 and apply Policy1 to the devices.

What can you protect by using Policy1?

- A. Microsoft Outlook
- B. Microsoft OneDrive
- C. Microsoft Teams
- D. Microsoft Edge

Answer: D

Question: 279

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage all Windows 11 devices.

You create an attack surface reduction (ASR) policy named Profile1 based on the Attack Surface Reduction Rules profile and assign Profile1 to all the devices.

A user reports that an Adobe Reader plug-in is now blocked.

You need to ensure that the plug-in is unblocked.

What should you do?

- A. Create an Endpoint Privilege Management policy and assign the policy to all the devices.
- B. Add a scope tag to Profile1.
- C. Configure ASR Only Per Rule Exclusions in Profile1.
- D. Create a device compliance policy and assign the policy to all the devices.

Answer: C

Question: 280

You have a Microsoft 365 E5 subscription.

All devices are enrolled in Microsoft Intune.

You need to ensure that devices that have NOT checked in for 30 days are deleted from Intune.

What should you configure from the Microsoft Intune admin center?

- A. a device limit restriction
- B. automatic enrollment
- C. a device clean-up rule
- D. a configuration profile

Answer: C

Question: 281

You have a Microsoft 365 E5 subscription.

All devices are enrolled in Microsoft Intune.

You create a Conditional Access policy named Policy1 that requires multifactor authentication (MFA).

You need to ensure that Policy1 only applies to devices marked as noncompliant.

Which settings of Policy1 should you configure?

- A. Device platforms under Conditions
- B. Filter for devices under Conditions
- C. Target resources
- D. Grant

Answer: B**Question: 282**

HOTSPOT

-

You have a Microsoft Entra tenant that contains the devices shown in the following table.

Name	Platform	Join type	Ownership
Device1	Windows 11	Microsoft Entra registered	Personal
Device2	Windows 10	Microsoft Entra joined	Corporate
Device3	Windows 11	Microsoft Entra joined	Corporate

The tenant contains the groups shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device3

You create a Windows Autopilot deployment profile as shown in the Deployment Profile exhibit. (Click the Deployment Profile tab.)

Create profile ...

Windows PC

- ✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Deployment1
Description	Deployment1 description
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Microsoft Entra ID as	Microsoft Entra joined
Skip AD connectivity check	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is registered for Autopilot.	<input type="radio"/>	<input type="radio"/>
Device2 is registered for Autopilot.	<input type="radio"/>	<input type="radio"/>
Device3 is registered for Autopilot.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Device1 is registered for Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is registered for Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is registered for Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 283

HOTSPOT

-

You have a Microsoft 365 tenant that uses Microsoft Intune to manage the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	Android Enterprise
Device4	iOS
Device5	iPadOS

You need to deploy a compliance solution that meets the following requirements:

- Marks the devices as Not Compliant if they do not meet compliance policies
- Remotely locks noncompliant devices

What is the minimum number of compliance policies required, and which devices support the remote lock action?
To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of compliance policies required:

▼

1

2

3

4

5

Devices that support the remote lock action:

▼

Device1 only

Device2 and Device3 only

Device4 and Device5 only

Device2, Device3, Device4, and Device5

Device1, Device2, Device3, Device4, and Device5

Answer:

Answer Area

Minimum number of compliance policies required:

▼

1

2

3

4

5

Devices that support the remote lock action:

▼

Device1 only

Device2 and Device3 only

Device4 and Device5 only

Device2, Device3, Device4, and Device5

Device1, Device2, Device3, Device4, and Device5

Question: 284

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain.

You have a Microsoft 365 E5 subscription that includes Microsoft Intune and syncs with the AD DS domain.

Windows Local Administrator Password Solution (Windows LAPS) is enabled in Microsoft Entra ID.

The subscription has the custom roles shown in the following table.

Name	Permission
Role1	microsoft.directory/deviceLocalCredentials/password/read
Role2	microsoft.directory/deviceLocalCredentials/standard/read
Role3	microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceLocalCredentials/password/read

Microsoft Entra contains the users shown in the following table.

Name	Built-in role	Assigned custom roles
User1	Helpdesk Administrator	Role1
User2	Security Reader	Role2
User3	None	Role3

You have the devices shown in the following table.

Name	Domain Join Type
Device1	Joined to AD DS
Device2	Microsoft Entra hybrid joined
Device3	Microsoft Entra joined

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	<input type="radio"/>	<input type="radio"/>
User2 can use Microsoft Entra to read the local administrator password of Device2.	<input type="radio"/>	<input type="radio"/>
User3 can use Microsoft Entra to read the local administrator password of Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can use Microsoft Entra to read the local administrator password of Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can use Microsoft Entra to read the local administrator password of Device3.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 285

HOTSPOT

-

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You purchase 50 Windows devices.

You configure automatic enrollment to Intune for Microsoft Entra joined devices.

You need to use a provisioning package to join the devices to Microsoft Entra.

What should you use to create the provisioning package, and what is the maximum amount of time you can use the package for bulk enrollment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use:

Intune Company Portal
Microsoft Deployment Toolkit (MDT)
Windows Configuration Designer
Windows Setup

Maximum amount of time:

30 days
90 days
180 days
365 days

Answer:

Answer Area

Use:

Intune Company Portal
Microsoft Deployment Toolkit (MDT)
Windows Configuration Designer
Windows Setup

Maximum amount of time:

30 days
90 days
180 days
365 days

Question: 286

You have a Microsoft 365 E5 subscription.

You need to configure the automated investigation and response (AIR) remediation level for a device named Device1 to require approval for all folders.

What should you create?

A.a security group

- B.a device group
- C.an administrative unit
- D.an action group

Answer: B

Question: 287

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You need to route Microsoft Intune logs to an Azure resource that supports the use of visuals, monitoring, and alerting.

Which settings should you configure in Intune, and which resource should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Settings:

▼

Connectors and tokens
Device diagnostics
Diagnostic settings
Intune add-ons

Resource:

▼

A Log Analytics workspace
An Azure logic app
A storage account
A virtual machine

Answer:

Answer Area

Settings:

▼

Connectors and tokens
Device diagnostics
Diagnostic settings
Intune add-ons

Resource:

▼

A Log Analytics workspace
An Azure logic app
A storage account
A virtual machine

Question: 288

HOTSPOT

-

You have a Microsoft 365 E5 subscription that includes Microsoft Intune.

You need to configure a compliance policy for the iOS/iPadOS platform. The solution must meet the following requirements:

- Require jailbroken devices to be marked as noncompliant.
- Mark devices without a password lock as noncompliant.

Which compliance policy settings should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Require jailbroken devices to be marked as noncompliant:

▼

Device Health
Device Properties
System Security

Require a password to unlock mobile devices:

▼

Device Health
Device Properties
System Security

Answer:

Answer Area

Require jailbroken devices to be marked as noncompliant:

▼

Device Health
Device Properties
System Security

Require a password to unlock mobile devices:

▼

Device Health
Device Properties
System Security

Question: 289

You have a Microsoft Intune subscription.

You have devices enrolled in Intune as shown in the following table.

Name	Operating system
Device1	Android 11
Device2	Android 12.1
Device3	iOS 12.3.1
Device4	iOS 12.3.2
Device5	iOS 13.5

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

- A.1
- B.2
- C.3
- D.4
- E.5

Answer: B

Question: 290

HOTSPOT

-

You have a Microsoft 365 E5 subscription. All devices are enrolled in Microsoft Intune.

You have a device group named Group1 that contains five Windows 11 devices.

You need to ensure that the devices in Group1 automatically receive new Windows 11 builds before the builds are released to the public.

What should you configure in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Profile type:

Feature updates for Windows 10 and later
Quality updates for Windows 10 and later
Update rings for Windows 10 and later

Prerelease channel:

Beta Channel
Dev Channel
Windows Insider -
Release Preview

Answer:

Answer Area

Profile type:

Feature updates for Windows 10 and later
Quality updates for Windows 10 and later
Update rings for Windows 10 and later

Prerelease channel:

Beta Channel
Dev Channel
Windows Insider -
Release Preview

Question: 291

HOTSPOT

-

You have a Microsoft 365 E5 subscription and use Microsoft Intune. The subscription contains a Microsoft Entra tenant that syncs with an on-premises Active Directory Domain Services (AD DS) domain. The tenant has Windows Local Administrator Password Solution (Windows LAPS) enabled.

You have the Windows devices shown in the following table.

Name	Join type	Enrolled in Intune
Device1	Joined to the AD DS domain	Yes
Device2	Microsoft Entra hybrid joined	Yes
Device3	Microsoft Entra joined	No

You have an Endpoint security policy that is configured as shown in the following table.

Setting	Value
Name	Policy1
Platform	Windows 10 and later
Profile	Local admin password solution (Windows LAPS)
Backup Directory	Backup the password to Azure AD only
Password Age Days	30
Assignments	Include: All devices

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The local administrator password of Device1 will be reset every 30 days.	<input type="radio"/>	<input type="radio"/>
The local administrator password of Device2 will be recoverable from Microsoft Entra ID.	<input type="radio"/>	<input type="radio"/>
The local administrator password of Device3 will be reset every 30 days.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
The local administrator password of Device1 will be reset every 30 days.	<input checked="" type="radio"/>	<input type="radio"/>
The local administrator password of Device2 will be recoverable from Microsoft Entra ID.	<input checked="" type="radio"/>	<input type="radio"/>
The local administrator password of Device3 will be reset every 30 days.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 292

You have a Microsoft Entra tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11.

You need to add Computer1 to contoso.com.

What should you use?

- A.the Settings app
- B.Computer Management
- C.netdom.exe

Answer: A

Question: 293

HOTSPOT

-

You have a Microsoft 365 subscription that includes Microsoft Intune.

From the Microsoft Intune admin center, you add the apps shown in the following table.

Name	Type	Operating system
App1	Microsoft 365 Apps for Windows 10 and later	Windows 10 and later
App2	Line-of-business (LOB) app	Android

You need to configure the apps to meet the following requirements:

- App1 must automatically install for all users in the marketing department on any Windows 11 device enrolled in Intune. If a user receives a new device, App1 must install automatically.
- App2 must be available for download for any user in the HR department from a personal Android device that is not enrolled in Intune.

Which assignment should you configure for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:

- A Required assignment to a device group
- A Required assignment to a user group
- An Available assignment to a device group
- An Available assignment to a user group

App2:

- A Required assignment to a device group
- A Required assignment to a user group
- An Available assignment to a device group
- An Available assignment to a user group

Answer:

Answer Area

App1:

- A Required assignment to a device group
- A Required assignment to a user group**
- An Available assignment to a device group
- An Available assignment to a user group

App2:

- A Required assignment to a device group
- A Required assignment to a user group
- An Available assignment to a device group
- An Available assignment to a user group**

Question: 294

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices that are joined to Microsoft Entra.

You purchase Microsoft 365 E5 licenses for all users.

You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

- A. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
- B. Subscription Activation
- C. an in-place upgrade by using Windows installation media
- D. Windows Autopilot

Answer: B

Question: 295

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in Microsoft Intune.

You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.

What should you do?

- A. From the Microsoft Intune admin center, add an app.
- B. From the Microsoft Intune admin center, create a Windows 10 and later device profile.
- C. From the Microsoft Entra admin center, add an enterprise application.

D.From the Microsoft Entra admin center, add an app registration.

Answer: A

Question: 296

You have a Microsoft 365 E5 subscription.

You have a Windows device named Device1 that is enrolled in Microsoft Intune.

On January 1,2024, you assign an app named App1 to Device1 as a required app.

The install of App1 fails.

What is the next date that Intune will attempt to install App1?

- A.January 2, 2024
- B.January 5, 2024
- C.January 8, 2024
- D.January 31, 2024

Answer: A

Question: 297

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Device3	Android	Microsoft Entra registered
Device4	iOS	Microsoft Entra registered

All the devices are enrolled in Microsoft Intune and have Microsoft 365 Apps for enterprise installed.

On which devices can you use the Cloud Policy service for Microsoft 365 to manage Microsoft 365 Apps for enterprise?

- A.Device2 only
- B.Device1 and Device2 only
- C.Device1, Device2, and Device3 only
- D.Device1, Device2, and Device4 only
- E.Device1, Device2, Device3, and Device4

Answer: E

Question: 298

HOTSPOT

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Device3	Android	Microsoft Entra registered

You install the Azure Monitor Agent on all supported devices.

You create a monitored object (MO) and associate the MO to a data collection rule (DCR) named DCR1.

You configure DCR1 as shown in the following exhibit.

Add data source ✕

* Data source

Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Performance Counters ✓

Choose Basic to enable the collection of performance counters.
Choose Custom if you want more control over which performance counters are collected.

None

Basic

Custom

☐

Performance counter

Sample rate (seconds)

☒

CPU

60

☒

Memory

60

☐

Disk

60

☐

Network

60

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
Azure Monitor collects CPU performance data from Device1.	<input type="radio"/>	<input type="radio"/>
Azure Monitor collects memory performance data from Device2.	<input type="radio"/>	<input type="radio"/>
Azure Monitor collects CPU performance data from Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Azure Monitor collects CPU performance data from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Azure Monitor collects memory performance data from Device2.	<input checked="" type="radio"/>	<input type="radio"/>
Azure Monitor collects CPU performance data from Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 299

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Microsoft Entra joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender for Endpoint on the computers.

You need to prevent users from disabling Microsoft Defender for Endpoint.

What should you do?

- A.From the Microsoft Intune admin center, create an attack surface reduction (ASR) policy.
- B.From the Microsoft Intune admin center, create an account protection policy.
- C.From the Microsoft Defender portal, enable tamper protection.
- D.From the Microsoft Intune admin center, create a device compliance policy.

Answer: C

Question: 300

You have a Microsoft 365 E5 subscription.

You need to manage operating system updates for corporate-owned Android Enterprise devices enrolled in Microsoft Intune.

What should you use?

- A.a compliance policy
- B.an Android FOTA deployment
- C.an Endpoint security policy
- D.a configuration profile

Answer: D

Question: 301

You have a Microsoft 365 subscription.

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

- A.the App1 deployment configurations
- B.a dynamic device group
- C.the App2 deployment configurations

Answer: C

Question: 302

HOTSPOT

-

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Multifactor authentication	Passwordless Capable	Methods Registered
User1	Capable	Not Capable	Mobile phone
User2	Capable	Not Capable	Software OATH token
User3	Capable	Not Capable	Microsoft Authenticator app (push notification), Software OATH token
User4	Capable	Capable	Microsoft Passwordless phone sign-in, Microsoft Authenticator app (push notification), Software OATH token

When you sign in to the tenant, the available verification methods are shown in the following exhibit.

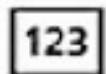
Verify your identity



Use a security key



Approve a request on my Microsoft Authenticator app



Use a verification code



Text +XXX XXXXXXXX65

Which users will be prompted for the verification code method, and which users will be prompted for the text method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Verification code:

▼

- User1 only
- User3 and User4 only
- User1, User3, and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

Text:

▼

- User1 only
- User3 and User4 only
- User1, User3, and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

Answer:

Verification code:

User1 only
User3 and User4 only
User1, User3, and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

Text:

User1 only
User3 and User4 only
User1, User3, and User4 only
User2, User3, and User4 only
User1, User2, User3, and User4

Question: 303

You have a Microsoft 365 subscription that contains Windows 11 devices enrolled in Microsoft Intune.

You need to use Device query to identify whether a critical security patch was installed on a device.

Which table should you target?

- A.WindowsQfe
- B.WindowsRegistry
- C.FileInfo
- D.OsVersion
- E.SystemInfo

Answer: A

Question: 304

You have a Microsoft 365 E5 subscription.

All Windows devices are enrolled in Microsoft Intune.

You need to deploy the Remote Help app to all the devices. The solution must minimize administrative effort.

Which type of app should you deploy?

- A.Windows app (Win32)
- B.line-of-business (LOB)
- C.Microsoft 365
- D.Microsoft Store

Answer: A

Question: 305

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra joined
Device2	Android	Microsoft Entra registered
Device3	macOS	Microsoft Entra registered

On which devices can you use Device query?

- A.Device1 only
- B.Device1 and Device2 only
- C.Device1 and Device3 only
- D.Device1, Device2, and Device3

Answer: A

Question: 306

You have a Microsoft 365 E5 subscription.

You need to use Device query to gather information about all the devices that are managed by using Microsoft Intune.

What should you do first?

- A.Enable Windows license verification.
- B.Onboard the devices to Microsoft Defender for Endpoint.
- C.Onboard the devices to Endpoint analytics.
- D.Create a compliance policy for all the devices.

Answer: C

Question: 307

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two devices named Device1 and Device2.

You manage the devices by using Microsoft Intune.

You need to use Device query to meet the following requirements:

- Identify the Windows build on a device.
- Validate whether a folder exists on the C drive of a device.

Which table should you target for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows build:

	▼
Cpu	
OSVersion	
SystemInfo	
WindowsService	

Folder:

	▼
DiskDrive	
FileInfo	
MemoryInfo	
SystemInfo	

Answer:

Windows build:

	▼
Cpu	
OSVersion	
SystemInfo	
WindowsService	

Folder:

	▼
DiskDrive	
FileInfo	
MemoryInfo	
SystemInfo	

Question: 308

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You plan to implement a Microsoft Cloud PKI solution that will deploy personal user certificates to all Windows

devices.

What is the minimum number of configuration profiles required to support the solution?

- A.1
- B.2
- C.3
- D.4

Answer: C

Question: 309

DRAG DROP

-

You have a Microsoft 365 subscription that contains the following devices enrolled in Microsoft Intune:

- A corporate-owned Windows device named Device1
- A personally-owned Android device named Device2

You need to use a remote action on each device. The solution must meet the following requirements:

- Repurpose Device1 by returning the device to the factory default settings.
- Remove only corporate data from Device2 and remove the device from Intune when the device checks in.

Which remote action should you use on each device? To answer, drag the appropriate remote actions to the correct devices. Each remote action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Remote actions

Delete

Fresh Start

Retire

Sync

Wipe

Answer Area

Device1:

Device2:

Answer:

Remote actions

Delete

Fresh Start

Retire

Sync

Wipe

Answer Area

Device1: Wipe

Device2: Retire

Question: 310

You have a Microsoft 365 E5 subscription.

You need to enroll Android Enterprise devices in Microsoft Intune by using zero-touch enrollment.

What should you do first?

- A.From the Microsoft Intune admin center, configure enrollment restrictions.
- B.From the Microsoft Intune admin center, create a zero-touch configuration.
- C.From the Microsoft Intune admin center, link a Managed Google Play account.
- D.From the zero-touch enrollment portal, create a zero-touch configuration.

Answer: C

Question: 311

You have a Microsoft Entra tenant named contoso.com that contains a group named Contoso Help Desk.

You need to ensure that Contoso Help Desk is added to the local Administrators group whenever a Windows device is joined to contoso.com.

What should you do?

- A.Assign the Cloud Device Administrator role to Contoso Help Desk.
- B.Assign the Microsoft Entra Joined Device Local Administrator role to Contoso Help Desk.
- C.Configure the Enterprise State Roaming settings.
- D.Enable Microsoft Entra Local Administrator Password Solution (LAPS) for contoso.com.

Answer: B

Question: 312

HOTSPOT

-

You have a Microsoft Entra tenant.

You are creating a dynamic device group named Group1.

Group1 will include only Windows devices that are Microsoft Entra registered.

How should you configure the dynamic membership rule for Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(device.deviceOSType -eq "Windows") and

device.deviceCategory
device.deviceOwnership
device.deviceTrustType
device.managementType

-eq

"AzureAd"
"ServerAd"
"Workplace"

)

Answer:

(device.deviceOSType -eq "Windows") and

device.deviceCategory
device.deviceOwnership
device.deviceTrustType
device.managementType

-eq

"AzureAd"
"ServerAd"
"Workplace"

)

Question: 313

DRAG DROP

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com. The subscription contains a user named User1 and a new Windows 11 device named Device1.

User1 must enroll Device1 in Microsoft Intune automatically.

You need to ensure that all other users cannot use automatic enrollment.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Enable Group1 to join devices to Microsoft Entra.

Create a group named Group1 and add User1 to Group1.

Configure the mobile device management (MDM) user scope.

Assign the Cloud Device Administrator role to User1.

Instruct User1 to register Device1 in contoso.com.

Add User1 as a device enrollment manager.

Instruct User1 to join Device1 to contoso.com.

Answer Area

1

2

3

Answer:

Actions

Enable Group1 to join devices to Microsoft Entra.

Create a group named Group1 and add User1 to Group1.

Configure the mobile device management (MDM) user scope.

Assign the Cloud Device Administrator role to User1.

Instruct User1 to register Device1 in contoso.com.

Add User1 as a device enrollment manager.

Instruct User1 to join Device1 to contoso.com.

Answer Area

1

2

3

Question: 314

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three Windows devices named Device1, Device2, and Device3.

Each device contains two apps named App1 and App2.

You manage the devices by using Microsoft Intune.

The subscription contains the groups shown in the following table.

Name	Members
Group1	Device1, Device3
Group2	Device2

You have an Endpoint Privilege Management (EPM) elevation settings policy named Policy1 that has the following settings:

- Endpoint Privilege Management: Enabled
- Default elevation response: Require user confirmation
- Validation: Windows authentication
- Assignments: Group1, Group2

You create an Endpoint Privilege Management elevation rules policy named RulesPolicy1 that has the following settings:

- Rule name: Rule1
- Elevation type: Automatic
- Child process behavior: Deny all
- File name: App1.exe
- Assignments: Group1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
A user on Device1 must provide credentials to run App2 with elevated access.	<input type="radio"/>	<input type="radio"/>
A user on Device2 can run App1 with elevated access without providing credentials.	<input type="radio"/>	<input type="radio"/>
A user on Device3 must provide credentials to run App1 with elevated credentials.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
A user on Device1 must provide credentials to run App2 with elevated access.	<input checked="" type="radio"/>	<input type="radio"/>
A user on Device2 can run App1 with elevated access without providing credentials.	<input type="radio"/>	<input checked="" type="radio"/>
A user on Device3 must provide credentials to run App1 with elevated credentials.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 315

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You need to deploy new Android devices as shown in the following table.

Name	Requirement
Device1	Must be shared by shift workers to perform warehouse inventory tracking
Device2	Must be assigned to a single user for work purposes only
Device3	Must support both work and personal use and enrollment by using a QR code

Which enrollment profile should you use for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Device2:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Device3:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Answer:

Device1:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Device2:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Device3:

Corporate-owned dedicated devices
Corporate-owned devices with work profile
Corporate-owned, fully managed user devices
Personally-owned devices with work profile

Question: 316

You have a Microsoft 365 subscription and use Microsoft Intune Suite.

The subscription contains devices enrolled in Intune as shown in the following table.

Name	Platform	Join type
Device1	Windows 10	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

Which devices support Device query?

- A.Device1 only
- B.Device2 only
- C.Device1 and Device2 only
- D.Device1, Device2, Device3, and Device4

Answer: A

Question: 317

You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune.

You plan to use Device query to provide on-demand information about the state of the devices. The solution must minimize costs.

What should you do first?

- A. Use the Collect diagnostics remote action.
- B. Purchase the Intune Advanced Analytics add-on.
- C. Purchase the Intune Suite add-on.
- D. Onboard the devices to Endpoint analytics.

Answer: D

Question: 318

You have a Microsoft Entra tenant that contains the devices shown in the following table.

Name	Platform	Join type	Microsoft Intune
Device1	Windows 11	Microsoft Entra joined	Enrolled
Device2	Windows 11	Microsoft Entra joined	Not enrolled
Device3	Windows 11	Microsoft Entra registered	Enrolled
Device4	Android	Microsoft Entra registered	Enrolled

On which devices can you implement Endpoint Privilege Management (EPM)?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device3, and Device4 only
- E. Device1, Device2, Device3, and Device4

Answer: A

Question: 319

HOTSPOT

-

You have a Microsoft 365 ES subscription and use Microsoft Intune Suite.

You manage the following types of devices:

- Windows 11
- Android
- iOS

You need to implement Microsoft Tunnel for Mobile Application Management (MAM) to provide the devices with access to on-premises company apps.

What should you deploy first, and which device types can use Tunnel for MAM? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Deploy:

- Intune Connector for Active Directory
- Microsoft Entra application proxy
- Microsoft Tunnel Gateway
- The Microsoft Authenticator app

Device types:

- Windows 11 only
- Windows 11 and Android only
- Windows 11 and iOS only
- Android and iOS only
- Windows 11, Android, and iOS

Answer:

Deploy:

- Intune Connector for Active Directory
- Microsoft Entra application proxy
- Microsoft Tunnel Gateway
- The Microsoft Authenticator app

Device types:

- Windows 11 only
- Windows 11 and Android only
- Windows 11 and iOS only
- Android and iOS only
- Windows 11, Android, and iOS

Question: 320

HOTSPOT

You have a Microsoft 365 subscription that includes Microsoft Intune and Microsoft Defender for Endpoint.

Users have devices that run Windows 11.

You deploy a connection from Defender for Endpoint to Intune.

You need to ensure that when a device is enrolled in Intune, the device is onboarded automatically to Defender for Endpoint.

What should you configure, and which portal should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure:

An account protection profile
An endpoint detection and response (EDR) profile
An onboarding package for Microsoft Defender

In portal:

Microsoft Defender portal
Microsoft Entra admin center
Microsoft Intune admin center

Answer:

Answer Area

Configure:

An account protection profile
An endpoint detection and response (EDR) profile
An onboarding package for Microsoft Defender

In portal:

Microsoft Defender portal
Microsoft Entra admin center
Microsoft Intune admin center

Question: 321

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra hybrid joined
Device2	Windows 11	Microsoft Entra joined
Device3	iOS	Microsoft Entra registered

The subscription contains the dynamic device groups shown in the following table.

Name	Dynamic membership rule
Group1	(device.deviceTrustType -eq "AzureAD") and (device.deviceOSType -eq "Windows")
Group2	(device.deviceTrustType -eq "Workplace")

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

Device1 is a member of Group1 only.

☐
☐

Device2 is a member of Group1 and Group2.

☐
☐

Device3 is a member of Group2 only.

☐
☐

Answer:

Answer Area

Statements

Yes

No

Device1 is a member of Group1 only.

☐
☒

Device2 is a member of Group1 and Group2.

☐
☒

Device3 is a member of Group2 only.

☒
☐

Question: 322

DRAG DROP

-

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Intune.

You need to meet the following requirements:

- Only allow the enrollment of devices that have a specific international mobile equipment identifier (IMEI).
- Support the enrollment and management of up to 1,000 devices.

Which enrollment setting should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Enrollment settings

CNAME Validation

Corporate device identifiers

Device enrollment managers

Device limit restriction

Device platform restriction

Answer Area

Only allow the enrollment of devices with a specific IMEI:

Support the enrollment and management of up to 1,000 devices:

Answer:

Enrollment settings

CNAME Validation

Corporate device identifiers

Device enrollment managers

Device limit restriction

Device platform restriction

Answer Area

Only allow the enrollment of devices with a specific IMEI:

Support the enrollment and management of up to 1,000 devices:

Corporate device identifiers

Device enrollment managers

Question: 323

HOTSPOT

-

You have a hybrid environment that contains a Microsoft Entra tenant and an on-premises Active Directory Domain Services (AD DS) domain. The environment contains the devices shown in the following table.

Name	Platform	Domain status
Device1	Windows 11	Workgroup
Device2	iOS	Not applicable

Which Microsoft Entra join type can each device use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:	<div>▼</div> <div>Microsoft Entra joined only Microsoft Entra registered only Microsoft Entra hybrid joined only Microsoft Entra joined or Microsoft Entra registered only Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined</div>
Device2:	<div>▼</div> <div>Microsoft Entra joined only Microsoft Entra registered only Microsoft Entra hybrid joined only Microsoft Entra joined or Microsoft Entra registered only Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined</div>

Answer:

Device1:	<div>▼</div> <div>Microsoft Entra joined only Microsoft Entra registered only Microsoft Entra hybrid joined only Microsoft Entra joined or Microsoft Entra registered only Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined</div>
Device2:	<div>▼</div> <div>Microsoft Entra joined only Microsoft Entra registered only Microsoft Entra hybrid joined only Microsoft Entra joined or Microsoft Entra registered only Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined</div>

Question: 324

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You need to ensure that only the members of Group1 can join devices to the Microsoft Entra tenant.

What should you configure in the Microsoft Entra admin center?

- A. Device settings
- B. Mobility
- C. Enterprise State Roaming
- D. User settings

Answer: A

Question: 325

You have a Microsoft Entra tenant named contoso.com that contains a Windows 11 device named Device1 and a user named User1.

User1 registers Device1 in contoso.com.

Which capability is available to Device1 after registering in contoso.com?

- A.authenticating to cloud resources by using single sign-on (SSO)
- B.enforcing compliance policies
- C.enforcing software updates
- D.enforcing hard drive encryption

Answer: A

Question: 326

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered

You need to create two dynamic device groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must contain Device1 and Device2 only.
- Group2 must contain Device1 and Device3 only.

Which device membership rule should you configure for each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Group1:

```
(device.deviceTrustType -eq "AzureAD")  
(device.displayName -eq "Device1") and (device.displayName -eq "Device2")  
(device.displayName -startsWith "Device") and (device.deviceOSType -eq "Windows")
```

Group2:

```
(device.deviceOSType -eq "iPhone") and (device.deviceOSType -eq "Windows")  
(device.deviceOSType -eq "iPhone") or (device.deviceOSType -eq "Windows")  
(device.deviceTrustType -eq "AzureAD") or (device.deviceOSType -eq "iPhone")
```

Answer:

Group1:

```
(device.deviceTrustType -eq "AzureAD")  
(device.displayName -eq "Device1") and (device.displayName -eq "Device2")  
(device.displayName -startsWith "Device") and (device.deviceOSType -eq "Windows")
```

Group2:

```
(device.deviceOSType -eq "iPhone") and (device.deviceOSType -eq "Windows")  
(device.deviceOSType -eq "iPhone") or (device.deviceOSType -eq "Windows")  
(device.deviceTrustType -eq "AzureAD") or (device.deviceOSType -eq "iPhone")
```

Question: 327

You have a Microsoft 365 E5 subscription.

You need to create a dynamic device group that will contain any device that has the word Marketing in its name.

Which device membership rule should you use?

- A.(device.displayName -in "Marketing")
- B.(device.displayName -in "*Marketing*")
- C.(device.displayName -contains "Marketing")
- D.(device.displayName -contains "*Marketing*")

Answer: C

Question: 328

You have a Microsoft 365 E5 subscription.

You need to ensure that when a Windows device is joined to the Microsoft Entra tenant, the device is enrolled automatically in Microsoft Intune.

What should you configure?

- A.the Windows Information Protection (WIP) user scope
- B.the Enterprise State Roaming settings
- C.the Microsoft Entra join and registration settings
- D.the mobile device management (MDM) user scope

Answer: D

Question: 329

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution: You use the Microsoft Intune Company Portal app.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 330

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution: You use Microsoft Entra Connect.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 331

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution: You use the Microsoft Authenticator app.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Question: 332

HOTSPOT

You have a Microsoft 365 E5 tenant that contains Windows devices enrolled in Microsoft Intune as shown in the following table.

Name	Member of	Join type
Device1	Group1, Group2	Microsoft Entra joined
Device2	Group2	Microsoft Entra joined
Device3	Group1, Group2	Microsoft Entra hybrid joined

You create an Endpoint Privilege Management (EPM) elevation settings policy named ElevationSettings1 that has the following settings:

- Endpoint Privilege Management: Enabled
- Default elevation response: Require user confirmation
- Validation: Business justification
- Assignments: Group1

Each device contains a file named File1.exe that can be run only by an administrator.

You create an EPM elevation rules policy named ElevationRules1 that has the following settings:

- Rule name: Rule1
- Elevation type: Automatic
- File name: File1.exe
- File hash:
- Assignments: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
A user on Device1 must provide a business justification to run File1.exe.	<input type="radio"/>	<input type="radio"/>
A user on Device2 can run File1.exe.	<input type="radio"/>	<input type="radio"/>
A user on Device3 can run File1.exe without providing a business justification.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements**Yes****No**

A user on Device1 must provide a business justification to run File1.exe.

☒☐

A user on Device2 can run File1.exe.

☒☐

A user on Device3 can run File1.exe without providing a business justification.

☐☒**Question: 333**

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Entra admin center, you assign the Helpdesk Administrator role to User1.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 334

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Intune admin center, you assign the Help Desk Operator role to User1.

Does this meet the goal?

A.Yes

B.No

Answer: A

Question: 335

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Intune admin center, you assign the Endpoint Security Manager role to User1.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 336

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Entra tenant named contoso.com.

You purchase an Android device named Device1.

You need to register Device1 in contoso.com.

Solution: You use the Google Chrome app.

Does this meet the goal?

A.Yes

B.No

Answer: B

Question: 337

You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune.

You need to review security tasks in the Microsoft Intune admin center.

What should you do first?

- A. Integrate Intune with Microsoft Defender for Endpoint.
- B. Implement the ServiceNow connector.
- C. Implement the Mobile Threat Defense connector.
- D. Deploy an attack surface reduction (ASR) policy.
- E. Deploy an Intune security baseline for Microsoft Defender for Endpoint.

Answer: A

Question: 338

You have a Microsoft 365 E5 subscription.

You purchase the following types of devices:

- Windows
- Android
- iOS

You plan to enroll the devices in Microsoft Intune.

You need to configure enrollment restrictions.

For which device types can you configure device manufacturer restrictions?

- A. Android only
- B. Windows only
- C. Android and iOS only
- D. Windows and iOS only
- E. Windows, Android, and iOS

Answer: A

Question: 339

HOTSPOT

-

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform	Join type	Mobile device management (MDM)
Device1	Windows 11	Microsoft Entra joined	None
Device2	Windows 11	Microsoft Entra registered	Microsoft Intune
Device3	Android	Microsoft Entra registered	Microsoft Intune

You need to use the remote actions shown in the following table.

Name	Action
Action1	Locate device
Action2	Remote lock

For each of the following statements, select Yes if the statement is true. Otherwise select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can use Action1 on Device1.	<input type="radio"/>	<input type="radio"/>
You can use Action2 on Device2.	<input type="radio"/>	<input type="radio"/>
You can use Action2 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can use Action1 on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
You can use Action2 on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
You can use Action2 on Device3.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 340

HOTSPOT

-

You have a Microsoft Entra tenant that contains the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2

The tenant contains the devices shown in the following table.

Name	Operating system
Device1	Windows 11
Device2	Windows 10
Device3	Windows 11

The devices have the enrollment restrictions shown in the following table.

Name	MDM	Personally owned devices	Minimum version	Included groups	Priority
Restriction1	Allow	Block	None	Group1	1
Restriction2	Allow	Allow	10.0.22000	Group1 Group2	2

For each of the following statements select yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User2 can enroll Device1 by using the Company Portal app.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device3 by using the Company Portal app.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User2 can enroll Device1 by using the Company Portal app.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 by using automatic enrollment.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device3 by using the Company Portal app.	<input type="radio"/>	<input checked="" type="radio"/>

You have a Microsoft Entra tenant that contains a device named Device1. Device1 is Microsoft Entra joined.

You need to validate the Microsoft Entra ID primary refresh token (PRT) for Device1.

Which command should you run?

- A.klist tgt
- B.dsregcmd /status
- C.query session
- D.sc.exe query state=all

Answer: B

Question: 342

Your on-premises network contains an Active Directory Domain Services (AD DS) domain that syncs with a Microsoft Entra tenant.

You need to enable users to connect to Microsoft 365 services from their personal Windows devices by using single sign-on (SSO). The solution must minimize organizational control of the devices.

Which join type should you use?

- A.Microsoft Entra registered
- B.Microsoft Entra joined
- C.Active Directory domain-joined
- D.Microsoft Entra hybrid joined

Answer: A

Question: 343

HOTSPOT

-

You have a Microsoft Entra tenant that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android
Device3	iOS
Device4	iPadOS

Which devices can be Microsoft Entra joined, and which devices can be Microsoft Entra registered? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra joined:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Microsoft Entra registered:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Answer:

Answer Area

Microsoft Entra joined:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Microsoft Entra registered:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Question: 344

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with a Microsoft Entra tenant named contoso.com.

You need to deploy 100 Windows 11 devices to contoso.com. The solution must meet the following requirements:

- Ensure that from the devices, users can access shares on an on-premises file server without being prompted for credentials.
- Minimize reliance on the on-premises infrastructure for device identity management.

Which join type should you use?

- A.Active Directory domain-joined
- B.Microsoft Entra hybrid joined
- C.Microsoft Entra joined
- D.Microsoft Entra registered

Answer: C

Question: 345

You have a Microsoft 365 E5 subscription that contains a device named Device1.

Device1 is Microsoft Entra joined.

You manage Device1 by using Microsoft Intune.

You need to use a remote action to reset the device as quickly as possible, if the device is turned off, the action must resume after the device is powered on.

Which remote action should you use?

- A.Autopilot reset
- B.Wipe
- C.Retire
- D.Delete

Answer: B

Question: 346

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android (personally-owned work profile)
Device3	iOS

You need to use a bulk device action to send custom notifications.

To which devices can you send the custom notifications?

- A.Device1 only
- B.Device2 only
- C.Device3 only
- D.Device2 and Device3 only
- E.Device1, Device2, and Device3

Answer: D

Question: 347

DRAG DROP

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You need to use Microsoft Cloud PKI to deploy personal user certificates to all Windows devices.

Which four actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Create device configuration SCEP certificate profiles.

Create an issuing certification authority (CA).

Create device configuration PKCS certificate profiles.

Create device configuration trusted certificate profiles.

Create a root certification authority (CA).

Create an account protection profile.

Create a Windows platform script.

Answer Area

Answer:

Answer Area

Create a root certification authority (CA).

Create an issuing certification authority (CA).

Create device configuration trusted certificate profiles.

Create device configuration SCEP certificate profiles.

Question: 348

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune Suite.

You need to recommend a solution that meets the following requirements:

- Administrators must use a secure connection over a shared screen session to perform remote tasks on a user's device.
- Administrators must have elevated access to perform remote tasks on a user's device.
- The solution must follow the principle of least privilege.

What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

For the connection, use:

Remote Desktop
Remote Help
Windows Remote Management (WinRM)

For elevated access, use:

Endpoint Privilege Manager
Help Desk Operator
Policy and Profile manager

Answer:

Answer Area

For the connection, use:

Remote Desktop
Remote Help
Windows Remote Management (WinRM)

For elevated access, use:

Endpoint Privilege Manager
Help Desk Operator
Policy and Profile manager

Question: 349

HOTSPOT

You have a Microsoft 365 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows
Device2	iOS
Device3	macOS

You plan to use the following remote actions on the devices:

- Collect diagnostics
- Locate device
- Remote lock

Which remote actions does each device support? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Device2:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Device3:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Answer:

Answer Area

Device1:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock**

Device2:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only**
- Collect diagnostics, Locate device, and Remote lock

Device3:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only**
- Collect diagnostics, Locate device, and Remote lock

Question: 350

You have a Microsoft 365 subscription and use Microsoft Intune Suite.

You plan to use Microsoft Cloud PKI to support the signing and encryption of email messages.

What should you do first?

- A.Create a root certification authority (CA).
- B.Create a device compliance policy.
- C.Create device configuration SCEP certificate profiles.
- D.Create device configuration trusted certificate profiles.
- E.Create an issuing certification authority (CA).

Answer: A

Question: 351

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Installed app	Microsoft Intune	Ownership
Device1	Android	Intune Company Portal Microsoft Edge	Not enrolled	<i>Not applicable</i>
Device2	iOS	Intune Company Portal	Enrolled	Personal

You need to implement Microsoft Tunnel for Mobile Application Management (MAM) to provide the devices with access to an on-premises web app named App1.

What should you do on each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

Enroll the device in Intune.
Install the Intune app.
Install the Microsoft Defender for Endpoint app.

Device2:

Change the Device Ownership property.
Install Edge.
Install the Microsoft Defender for Endpoint app.

Answer:

Answer Area

Device1:

Enroll the device in Intune.
Install the Intune app.
Install the Microsoft Defender for Endpoint app.

Device2:

Change the Device Ownership property.
Install Edge.
Install the Microsoft Defender for Endpoint app.

You have a Microsoft 365 subscription.

You plan to enroll 25 new devices in Microsoft Intune.

You need to configure an enrollment notification for the new devices.

Which two types of notifications can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.SMS

B.Microsoft Teams message

C.phone call

D.push

E.email

Answer: DE

Question: 353

HOTSPOT

-

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Role
Admin1	None	Global Administrator
User1	Group1	None

For contoso.com, you configure the following Microsoft Entra join and registration settings:

- Users may join devices to Microsoft Entra: Selected
- o Selected: Group1

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can join Device1 to contoso.com.	<input type="radio"/>	<input type="radio"/>
User1 can join Device2 to contoso.com.	<input type="radio"/>	<input type="radio"/>
User1 can join Device3 to contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can join Device1 to contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can join Device2 to contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can join Device3 to contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 354

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains a Windows device named Device1.

Device1 was onboarded to Microsoft Defender for Endpoint by using a local script.

You use Microsoft Intune to manage Device1.

You plan to use the machine risk score in a compliance policy.

You need to ensure that the machine risk score is evaluated based on data from Defender for Endpoint.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

From the Endpoints settings of the Microsoft Defender portal:

Configure the Advanced features settings.
Configure the Intune Permissions settings.
Select Onboarding, and then configure the Deployment method setting.

From the Microsoft Intune admin center:

Create a Configuration profile.
Configure the Compliance settings.
Configure the Microsoft Defender for Endpoint settings.

Answer:

Answer Area

From the Endpoints settings of the Microsoft Defender portal:

Configure the Advanced features settings.
Configure the Intune Permissions settings.
Select Onboarding, and then configure the Deployment method setting.

From the Microsoft Intune admin center:

Create a Configuration profile.
Configure the Compliance settings.
Configure the Microsoft Defender for Endpoint settings.

Question: 355

HOTSPOT

-

You have a Microsoft 365 subscription and use Microsoft Intune.

You have the Endpoint Privilege Management (EPM) elevation settings policy shown in the following exhibit.

✓ Basics **2 Configuration settings** 3 Scope tags 4 Assignments 5 Review + create

^ Privilege Management Elevation Client Settings

Elevation settings establish the default behaviors for the endpoint elevation client.

Endpoint Privilege Management ☒ Enabled

Default elevation response Not configured

Send elevation data for reporting * Yes

Reporting scope * Diagnostic data and managed elevations only

No EPM elevation rules policies are configured.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Software installations will [answer choice].

be denied.
require support approval.
require user confirmation.

[Answer choice] will be reported.

All diagnostic data and elevations
No diagnostic data or elevations
Only diagnostic data

Answer:

Answer Area

Software installations will [answer choice].

be denied.
require support approval.
require user confirmation.

[Answer choice] will be reported.

All diagnostic data and elevations
No diagnostic data or elevations
Only diagnostic data

Question: 356

You have a Microsoft 365 E5 subscription that contains the following types of devices:

- Windows 11
- Android
- iOS

All the devices are enrolled in Microsoft Intune.

You need to use Intune to deploy apps from the Enterprise App Catalog.

To which device types can you deploy the apps?

- A.Windows 11 only
- B.Windows 11 and Android only
- C.Windows 11 and is only
- D.Android and iOS only
- E.Windows 11, Android, and iOS

Answer: A

Question: 357

You have a Microsoft 365 E5 subscription and use Microsoft Intune Suite.

You plan to use Intune to run remediation script packages.

What should you do first in the Microsoft Intune admin center?

- A.Enable Windows diagnostic data in processor configuration.
- B.Enable Windows license verification.
- C.Configure the Derived Credential settings.
- D.Upload a Windows enterprise certificate.

Answer: B

Question: 358

HOTSPOT

-

You have a Microsoft 365 subscription that contains 5,000 Windows devices enrolled in Microsoft Intune.

You plan to use the Sync and Collect diagnostics bulk device actions.

What is the maximum number of devices you can include in each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sync:

	▼
25	
50	
100	
500	
1000	

Collect diagnostics:

	▼
25	
50	
100	
500	
1000	

Answer:

Answer Area

Sync:

Collect diagnostics:

25
50
100
500
1000

25
50
100
500
1000

Question: 359

HOTSPOT

-

You manage devices by using Microsoft Intune. Automatic Intune enrollment is disabled.

Users report that they must enter the mobile device management (MDM) server address during device enrollment.

To reduce user interaction during device enrollment, you plan to create the following CNAME DNS hostname records:

- EnterpriseEnrollment.contoso.com
- EnterpriseRegistration.contoso.com

You need to configure a fully qualified domain name (FQDN) for each CNAME record to redirect enrollment requests to the Intune servers.

How should you configure each FQDN? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

EnterpriseEnrollment-s

.cloud.microsoft
.manage.microsoft.com
.onmicrosoft.com
.windows.net

EnterpriseRegistration

.cloud.microsoft
.manage.microsoft.com
.onmicrosoft.com
.windows.net

Answer:

Answer Area

EnterpriseEnrollment-s

.cloud.microsoft
.manage.microsoft.com
.onmicrosoft.com
.windows.net

EnterpriseRegistration

.cloud.microsoft
.manage.microsoft.com
.onmicrosoft.com
.windows.net

Question: 360

You have a Microsoft 365 E5 subscription and use Microsoft Intune.

You need to use a Sync bulk device action on all corporate-owned Windows devices.

What is the maximum number of devices you can include the action?

- A.25
- B.50
- C.100
- D.500
- E.1000

Question: 361

HOTSPOT

-

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
Admin3	Directory Writer
User1	<i>None</i>

The tenant contains a standalone workgroup computer named Computer1 that runs Window 11. Computer1 contains the local users shown in the following table.

Name	Member of
UserA	Administrators
UserB	Power Users
UserC	Device Owners
UserD	Users

Computer1 needs to be joined to contoso.com.

Which local users can join Computer1 to contoso.com, and the Microsoft Entra credentials of which user can be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Local users:

UserA only
UserA or UserB only
UserA or UserC only
UserA, UserB, or UserC only
UserA, UserB, UserC, or UserD

Credentials of:

Admin1 only
Admin1 or Admin2 only
Admin1 or Admin3 only
Admin1, Admin2, or Admin3 only
Admin1, Admin2, Admin3, or User1

Answer:

Answer Area

Local users:

UserA only
UserA or UserB only
UserA or UserC only
UserA, UserB, or UserC only
UserA, UserB, UserC, or UserD

Credentials of:

Admin1 only
Admin1 or Admin2 only
Admin1 or Admin3 only
Admin1, Admin2, or Admin3 only
Admin1, Admin2, Admin3, or User1

Question: 362

HOTSPOT

You have a Microsoft Entra tenant named contoso.com that contains the dynamic membership groups shown in the following table.

Name	Dynamic membership rule
Group1	(device.displayName -startsWith "Dev") or (device.deviceOSType -eq "Android")
Group2	(device.deviceTrustType -eq "workplace")
Group3	(device.deviceTrustType -eq "AzureAD") and (device.deviceOSType -eq "Android")

You add devices to contoso.com as shown in the following table.

Name	Platform	Join type
Device1	Windows	Microsoft Entra joined
Device2	Windows	Microsoft Entra registered
Phone1	Android	Microsoft Entra registered

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

Device1 is a member of Group1 only.

☐☐

Device2 is a member of Group1 and Group2.

☐☐

Phone1 is a member of Group1 and Group3.

☐☐

Answer:

Answer Area

Statements

Yes

No

Device1 is a member of Group1 only.

☒☐

Device2 is a member of Group1 and Group2.

☒☐

Phone1 is a member of Group1 and Group3.

☐☒

Question: 363

You have a Microsoft 365 E5 subscription.

You have a Microsoft Intune enrollment profile for Android Enterprise devices that has the following settings:

- Name: Profile1
- Token type: Corporate-owned, fully managed

You need to enroll a new Android device in Intune by using Profile1.

What should you use to enroll the device?

- A.a QR code
- B.the Company Portal app
- C.the Microsoft Authenticator app
- D.the Intune app

Answer: A

Question: 364

You use Microsoft Defender for Office 365.

You plan to automate an attack simulation campaign.

Any users that fail the simulation must take additional training based on the simulation results.

What is the maximum number of days the training will be available to the users after the simulation?

- A.7
- B.15
- C.30
- D.45

Answer: C

Question: 365

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

The subscription contains users that have devices onboarded to Microsoft Defender for Endpoint. Defender for Endpoint is configured to forward signals to Microsoft Defender for Cloud Apps.

Cloud Discovery identifies a risky web app named App1.

You need to block users from connecting to App1 from Microsoft Edge. Users must be able to bypass the restriction.

Which type of app tag should you use, and what should you configure to integrate Defender for Endpoint with Defender for Cloud Apps? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App tag type:

▼

Monitored
Sanctioned
Unsanctioned

Integrate by configuring:

▼

Anonymization
Asset rule management
Enforce app access

Answer:

Answer Area

App tag type:

Monitored
Sanctioned
Unsanctioned

Integrate by configuring:

Anonymization
Asset rule management
Enforce app access

Question: 366

You have a Microsoft 365 E5 subscription and use Microsoft Defender for Cloud Apps.

You plan to perform a security audit of all the apps detected by Cloud Discovery.

You need to track which apps were audited. The solution must ensure that the list of audited apps can be displayed in the cloud app catalog.

What should you do?

- A. Apply a custom app tag to each app.
- B. Deploy Conditional Access App Control.
- C. Define each app as a critical asset.
- D. Generate a Cloud Discovery snapshot report.
- E. Enable app governance.

Answer: A

Question: 367

You have a Microsoft 365 E5 subscription that contains Windows 11 devices.

All the devices are onboarded to Microsoft Defender for Endpoint.

You need to compare the configuration of the devices against industry standard benchmarks.

What should you use?

- A. Attack surface map
- B. Events
- C. Security baselines assessment
- D. Initiatives

Answer: C

Question: 368

HOTSPOT

-

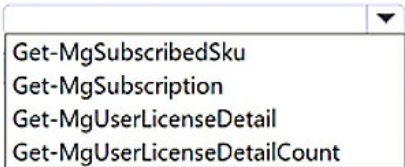
You have a Microsoft 365 E5 subscription.


You need to use Microsoft Graph PowerShell to assign a Microsoft 365 E5 license to a new user named .

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

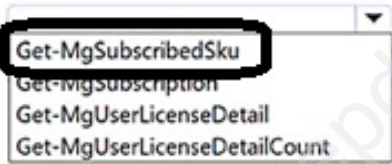
Answer Area


\$e5Sku =  -All | Where SkuPartNumber -eq 'SPE_E5'

 -UserId "user1@contoso.com" -AddLicenses @{SkuId = \$e5Sku.SkuId} -RemoveLicenses @()

Answer:

Answer Area

\$e5Sku =  -All | Where SkuPartNumber -eq 'SPE_E5'

 -UserId "user1@contoso.com" -AddLicenses @{SkuId = \$e5Sku.SkuId} -RemoveLicenses @()

Question: 369

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You plan to create a Conditional Access policy named Policy1.

You need to ensure that only Passwordless MFA authentication methods are used when administrators attempt to access the Azure portal, Azure PowerShell, or Azure Command-Line Interface (CLI).

How should you configure Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Access controls:

Set Grant to Require authentication strength.
Set Grant to Require multifactor authentication.
Set Session to Use app enforced restrictions.
Set Session to Use Conditional Access App Control.

Target resources:

Azure Credential Configuration Endpoint Service
Windows Azure Service Management API
Windows Cloud Login

Answer:

Answer Area

Access controls:

Set Grant to Require authentication strength.
Set Grant to Require multifactor authentication.
Set Session to Use app enforced restrictions.
Set Session to Use Conditional Access App Control.

Target resources:

Azure Credential Configuration Endpoint Service
Windows Azure Service Management API
Windows Cloud Login

Question: 370

HOTSPOT

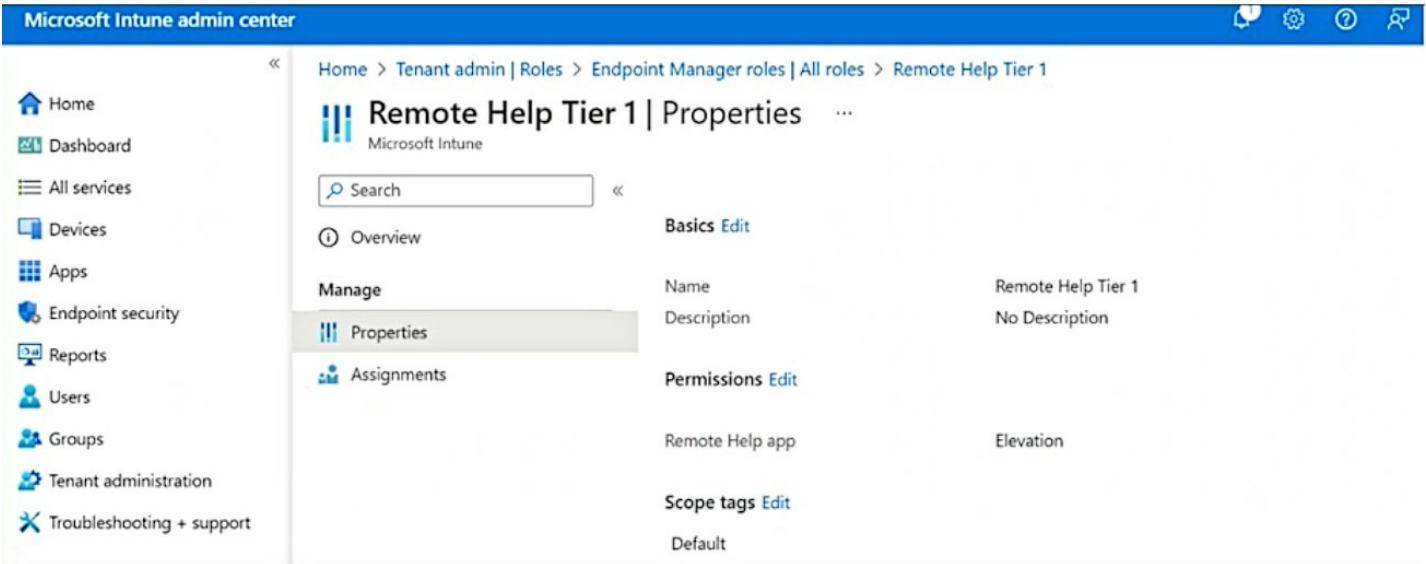
You have a Microsoft 365 E5 subscription that contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	iOS
Device3	Android

The subscription contains the users shown in the following table.

Name	Role	Role type
Admin1	Help Desk Operator	Built-in role
Admin2	Remote Help Tier1	Custom Intune role

The Remote Help Tier1 role is configured as shown in the following exhibit.



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 can take full control of Device2.	<input type="radio"/>	<input type="radio"/>
Admin2 can take full control of Device1.	<input type="radio"/>	<input type="radio"/>
Admin2 can take unattended control of Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can take full control of Device2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can take full control of Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can take unattended control of Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 371

HOTSPOT

-

You have a Microsoft 365 subscription and use the Microsoft Intune Suite.
You have the devices shown in the following table.

Name	Platform	Version
Device1	iOS	13.7
Device2	Android	13
Device3	iOS	15.8.3

You plan to implement Microsoft Tunnel for Mobile Application Management (MAM).

Which types of tunnels are supported by the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tunnel for MAM:

Device2 only
Device3 only
Device1 and Device2 only
Device1 and Device3 only
Device2 and Device3 only
Device1, Device2, and Device3

A per-app VPN tunnel:

Device2 only
Device3 only
Device1 and Device2 only
Device1 and Device3 only
Device2 and Device3 only
Device1, Device2, and Device3

Answer:

Answer Area

Tunnel for MAM:

Device2 only
Device3 only
Device1 and Device2 only
Device1 and Device3 only
Device2 and Device3 only
Device1, Device2, and Device3

A per-app VPN tunnel:

Device2 only
Device3 only
Device1 and Device2 only
Device1 and Device3 only
Device2 and Device3 only
Device1, Device2, and Device3

Question: 372

HOTSPOT

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
User1	<i>None</i>

You purchase the devices shown in the following table.

Name	Operating system
Device1	Windows 11
Device2	Windows 10

Administrators perform the following actions:

- Join Device1 to contoso.com by using the credentials of Admin1.
- Register Device2 in contoso.com by using the credentials of Admin2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The Admin2 credentials can be used to sign in to Device1.	<input type="radio"/>	<input type="radio"/>
The Admin2 credentials can be used to sign in to Device2.	<input type="radio"/>	<input type="radio"/>
The credentials of User1 can be used to sign in to Device1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area		
Statements	Yes	No
The Admin2 credentials can be used to sign in to Device1.	<input checked="" type="radio"/>	<input type="radio"/>
The Admin2 credentials can be used to sign in to Device2.	<input type="radio"/>	<input checked="" type="radio"/>
The credentials of User1 can be used to sign in to Device1.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 373

SIMULATION

Username and password

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

Microsoft 365 Password: i7A4\$3o^HGD3L~=c[9xuOhM%^4:s11Ai

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://portal.office.com”, and press Enter.

The following information is for technical support purposes only:

You need to create a compliance policy to validate whether all the Windows 10 or later devices enrolled in Microsoft Intune have BitLocker Drive Encryption (BitLocker) enabled.

Answer:

Manage Disk Encryption policy for Windows devices with Intune

Create an endpoint security policy for Windows

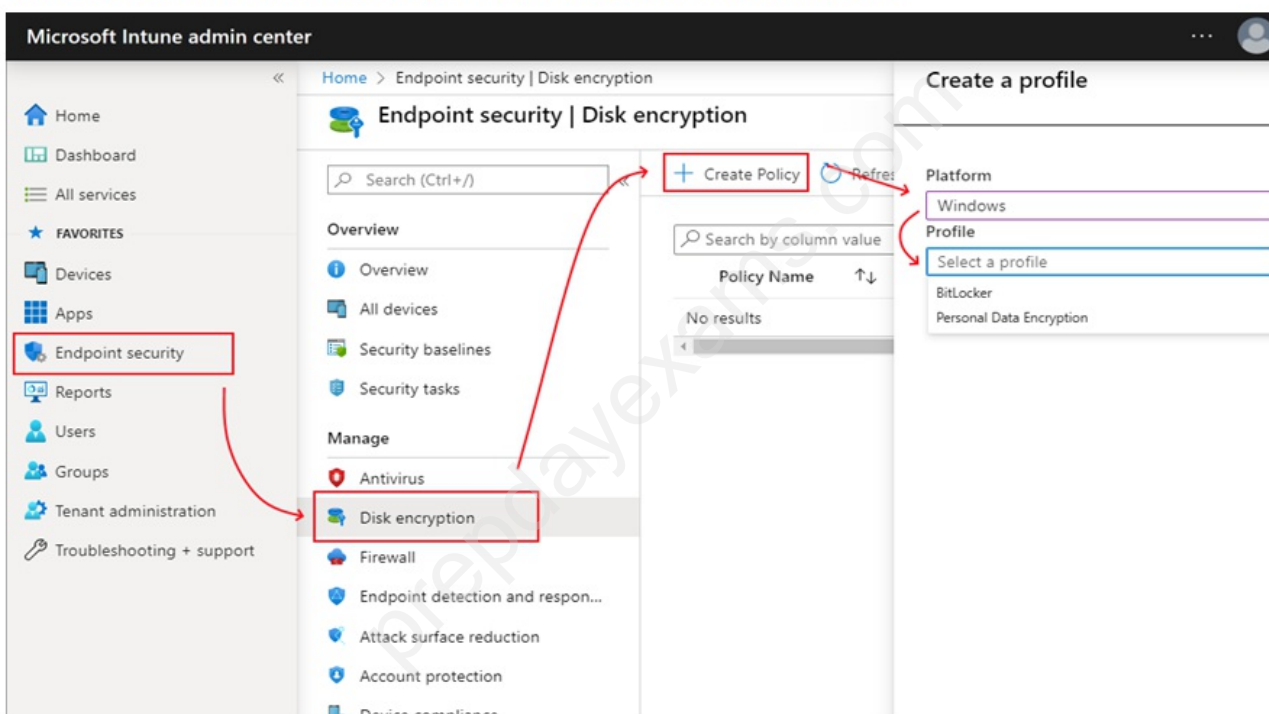
Step 1: Sign in to the Microsoft Intune admin center.

Step 2: Select Endpoint security > Disk encryption > Create Policy.

Step 3: Set the following options:

Platform: Windows

Profile: Choose either BitLocker or Personal Data Encryption [Choose BitLocker]



Step 4: On the Configuration settings page, configure settings for BitLocker to meet your business needs. [Skip]

Select Next.

Step 5: On the Scope (Tags) page, choose Select scope tags to open the Select tags pane to assign scope tags to the profile. [Skip]

Select Next to continue.

Step 6: On the Assignments page, select the groups that receive this profile. [Skip]

Select Next.

Step 7: On the Review + create page, when you're done, choose Create. The new profile is displayed in the list when you select the policy type for the profile you created.

Reference:

<https://learn.microsoft.com/en-us/intune/intune-service/protect/encrypt-devices>

Question: 374

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

Microsoft 365 Password: i7A4\$3o^HGD3L~=c[9xuOhM%^4:s11Ai

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://portal.office.com”, and press Enter.

The following information is for technical support purposes only:

Lab Instance: 48262079

-

You need to ensure that when the members of a group named sg-Engineering join their Windows devices to Microsoft Entra, the devices are enrolled automatically in Microsoft Intune. The solution must affect only the sg-Engineering group members.

Answer:

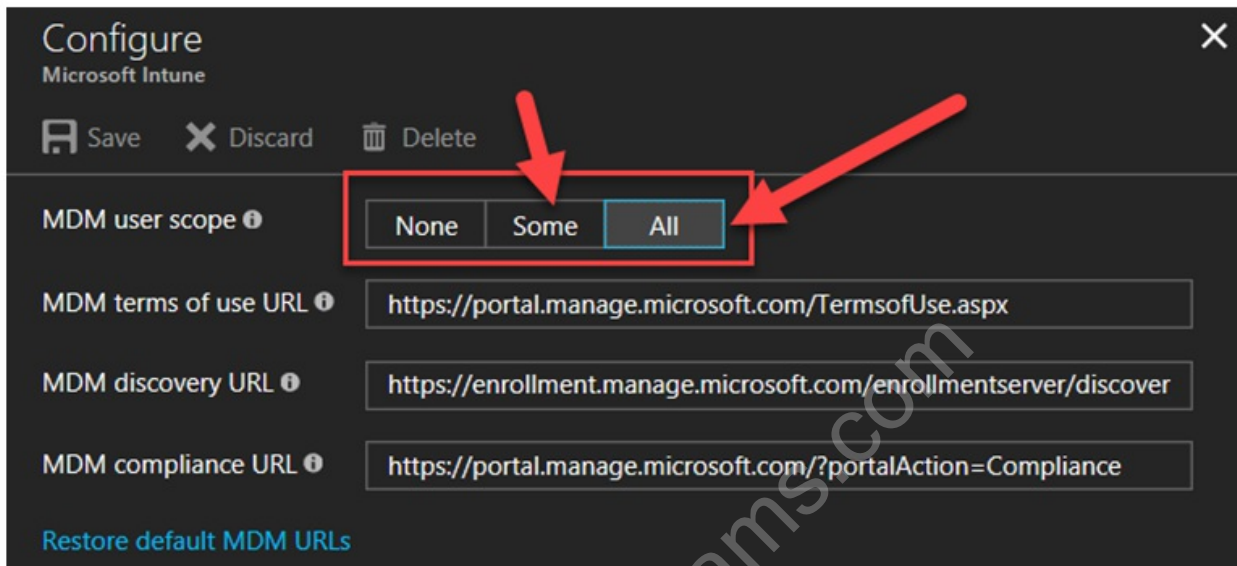
Automatic MDM enrollment in the Intune admin center

Windows devices can be enrolled in to Intune automatically when they join or register with Microsoft Entra ID. Automatic enrollment can be configured in Azure portal.

Step 1: Go to your Microsoft Entra admin center.

Step 2: Select Mobility (MDM and MAM), and find the Microsoft Intune app.

Step 3: Select Microsoft Intune and configure the enrollment options. You can specify settings to allow All users to enroll a device, or choose to allow Some users (and specify a group).



The screenshot shows the 'Configure' window for Microsoft Intune. At the top, there are buttons for 'Save', 'Discard', and 'Delete'. Below these, the 'MDM user scope' section is highlighted with a red box. Inside this box, there are three radio button options: 'None', 'Some', and 'All'. The 'All' option is selected. Two red arrows point to the 'Some' and 'All' options. Below the radio buttons, there are three text input fields for MDM URLs: 'MDM terms of use URL' (https://portal.manage.microsoft.com/TermsofUse.aspx), 'MDM discovery URL' (https://enrollment.manage.microsoft.com/enrollmentserver/discover), and 'MDM compliance URL' (https://portal.manage.microsoft.com/?portalAction=Compliance). At the bottom left, there is a link 'Restore default MDM URLs'.

Step 4: Click Some.

Step 5: Select the sg-Engineering Group.

Step 6: Select Save to configure MDM autoenrollment for Microsoft Entra joined devices and bring-your-own-device scenarios.

Reference:

<https://learn.microsoft.com/sv-se/windows/client-management/azure-ad-and-microsoft-intune-automatic-mdm-enrollment-in-the-new-portal>

Question: 375

SIMULATION

-

Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and select the username below.

To enter your password, place your cursor in the Enter password box and select the password below.

Microsoft 365 Username:

Microsoft 365 Password: i7A4\$3o^HGD3L~=c[9xuOhM%^4:s11Ai

If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL “https://portal.office.com”, and press Enter.

The following information is for technical support purposes only:

Lab Instance: 48262079

-

You need to create an endpoint security policy to turn on Windows SmartScreen for all Windows devices.

Answer:

Step 1: Sign in to the Microsoft Intune admin center.

Create an endpoint security policy

The following procedure provides general guidance for creating endpoint security policies:

1. Sign in to the Microsoft Intune admin center. [Step 1]

Step 2: Select Endpoint security and then select the type of policy you want to configure [Select Application control], and then select Create Policy.

2. Select Endpoint security and then select the type of policy you want to configure, and then select Create Policy. Choose from the following policy types:

Account protection

Antivirus

*-> Application control (Preview) [Step 2]

Attack surface reduction

Disk encryption

Endpoint detection and response

Firewall

Step 3: For Platform select Windows.

3. Enter the following properties:

Platform: Choose the platform that you're creating policy for. The available options depend on the policy type you select.

Profile: Choose from the available profiles for the platform you selected. For information about the profiles, see the dedicated section in this article for your chosen policy type.

Step 4: Select Create.

Step 5: On the Basics page, enter a name and description for the profile, then choose Next.

Step 6: On the Configuration settings page, expand each group of settings, and configure the settings you want to manage with this profile.

Here: Turn on Windows SmartScreen

When your done configuring settings, select Next.

Step 7: On the Scope tags page, choose Select scope tags to open the Select tags pane to assign scope tags to the profile.

Select Next to continue.

Step 8: On the Assignments page, select the groups that will receive this profile.

Select Next.

Step 9: On the Review & create page, select Create. The name you enter is displayed in the list when you select the

Step 9: On the Review + create page, when you're done, choose Create. The new profile is displayed in the list when you select the policy type for the profile you created.

Note:

Attack surface reduction policy settings for endpoint security in Intune

View the settings you can configure in profiles for Attack surface reduction policy in the endpoint security node of Intune as part of an Endpoint security policy.

Application control profile

Microsoft Defender Application Control

* App locker application control

* Block users from ignoring SmartScreen warnings

*-> Turn on Windows SmartScreen

--

Following are brief descriptions of each endpoint security policy type.

* App Control for Business (Preview) - Manage approved apps for Windows devices with App Control for Business policy and Managed Installers for Microsoft Intune. Intune App Control for Business policies are an implementation of Windows Defender Application Control (WDAC).

* Etc. [Many other]

Reference:

<https://learn.microsoft.com/en-us/intune/intune-service/protect/endpoint-security-policy>

<https://learn.microsoft.com/en-us/intune/intune-service/protect/endpoint-security-asr-profile-settings>

Question: 376

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three Windows devices named Device1, Device2, and Device3. The devices are managed by using Microsoft Intune. Each device contains a file named Script1.ps1.

Users do NOT have local administrator permissions for the devices.

The subscription contains the groups shown in the following table.

Name	Member
Group1	Device1
Group2	Device2
Group3	Device3

You create two Endpoint Privilege Management (EPM) elevation settings policies that have the following settings:

•Name: Policy1

•Endpoint Privilege Management: Enabled

oDefault elevation response: Deny all requests

oAllow Elevation Detection: No

oSend elevation data for reporting: No

•Assignments:

oIncluded groups: Group1

•Name: Policy2

•Endpoint Privilege Management: Require support approval

oAllow Elevation Detection: No

oSend elevation data for reporting: No

•Assignments:

oIncluded groups: Group3

You create an EPM elevation rules policy named RulesPolicy1 that has the following settings:

- Rule name: Rule1
- oElevation type: Automatic
- oChild process behavior: Deny all
- oFile name: Script1.ps1
- oFile hash:
- Assignments: Group 1, Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
A user on Device1 must get approval before the user can run Script1.ps1 with elevated privileges.	<input type="radio"/>	<input type="radio"/>
A user on Device2 must get approval before the user can run Script1.ps1 with elevated privileges.	<input type="radio"/>	<input type="radio"/>
A user on Device3 must get approval before the user can run Script1.ps1 with elevated privileges.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
A user on Device1 must get approval before the user can run Script1.ps1 with elevated privileges.	<input type="radio"/>	<input checked="" type="radio"/>
A user on Device2 must get approval before the user can run Script1.ps1 with elevated privileges.	<input type="radio"/>	<input checked="" type="radio"/>
A user on Device3 must get approval before the user can run Script1.ps1 with elevated privileges.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 377

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.

You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Entra admin center, you assign the Cloud Device Administrator role to User1.

Does this meet the goal?

- A.Yes
- B.No

Answer: B

Question: 378

You have a Microsoft 365 subscription and use the Microsoft Intune Suite.

You have the devices shown in the following table.

Name	Platform	Join type
Device1	Windows	Microsoft Entra joined
Device2	Windows	Microsoft Entra hybrid joined
Device3	Windows	Microsoft Entra registered
Device4	macOS	Microsoft Entra registered

All the devices are enrolled in Intune.

Which devices can you query by using Device query?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Answer: B

Question: 379

HOTSPOT

-

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You have the devices shown in the following table.

Name	Platform	Description
Device1	Windows 11	Workgroup
Device2	macOS	Microsoft Entra registered
Device3	Android	Microsoft Entra registered

The Windows Enrollment settings have the following configurations:

- MDM user scope: Group1
- Windows Information Protection (WIP) user scope: Group2

You configure Microsoft Intune enrollment restrictions as shown in the exhibit. (Click the Exhibit tab.)

All services > Devices | Enrollment > Enrollment restrictions > All Users | Properties >

Edit restriction

Device type restriction

Platform settings

Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more](#)

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	<div>Manufacturer name here, he...</div>
Android device administrator	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	<div>Manufacturer name here, he...</div>
iOS/iPadOS	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	Restriction not supported
macOS	<div>AllowBlock</div>	Restriction not supported	<div>AllowBlock</div>	Restriction not supported
Windows (MDM) ⓘ	<div>AllowBlock</div>	Allow min/max range: <div>MinMax</div>	<div>AllowBlock</div>	Restriction not supported

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune.	<input type="radio"/>	<input type="radio"/>
User3 can enroll Device3 in Intune.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll Device3 in Intune.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 380

You have a Microsoft 365 subscription that contains 500 Android devices. The devices are managed by using Microsoft Intune.

You need to ensure that you can manage software updates for the devices by using Android FOTA.

What should you do first?

- A. Create a compliance policy.
- B. Add a compliance partner.
- C. Configure a connector.
- D. Add derived credentials.

Answer: C

Question: 381

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains 500 Windows devices and the resources shown in the following table.

Name	Description
User1	User
Group1	Security group
Device1	Windows device enrolled in Microsoft Intune
Device2	Microsoft Entra joined Windows device

Both devices have Microsoft 365 apps installed.

You need to create and assign a Policies for Office Apps policy that will block macros from running in Office files from the internet.

Which portal should you use, and what is the scope of the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal:

- The Microsoft Intune admin center only
- The Microsoft 365 Apps admin center only
- The Microsoft Intune admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center and Microsoft 365 Apps admin center only
- The Microsoft 365 Apps admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center, Microsoft 365 Apps admin center and Microsoft 368 admin center

Scope:

- Device1 only
- Group1 only
- Device1 and Device2 only
- Group1 and User1 only
- Device1, Group1, and User1 only
- Device1, Device2, Group1 and User1

Answer:

Answer Area

Portal:

- The Microsoft Intune admin center only
- The Microsoft 365 Apps admin center only
- The Microsoft Intune admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center and Microsoft 365 Apps admin center only**
- The Microsoft 365 Apps admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center, Microsoft 365 Apps admin center and Microsoft 368 admin center

Scope:

- Device1 only
- Group1 only
- Device1 and Device2 only
- Group1 and User1 only
- Device1, Group1, and User1 only
- Device1, Device2, Group1 and User1**

Question: 382

You have a Microsoft 365 E5 subscription.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android
Device3	iOS
Device4	macOS

Which devices can be enrolled in Microsoft Intune by using automatic enrollment?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3 only
- E. Device1, Device2, Device3, and Device4

Answer: E

Question: 383

HOTSPOT

-

You have a hybrid environment that contains a Microsoft Entra tenant and an on-premises Active Directory Domain Services (AD DS) domain.


You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	iOS

Which Microsoft Entra join type can each device use? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

Device1: 


Microsoft Entra joined only

Microsoft Entra registered only

Microsoft Entra hybrid joined only

Microsoft Entra joined or Microsoft Entra registered only

Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Device2: 

Microsoft Entra joined only

Microsoft Entra registered only


Microsoft Entra hybrid joined only

Microsoft Entra joined or Microsoft Entra registered only

Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Answer:

Answer Area

Device1: 


Microsoft Entra joined only

Microsoft Entra registered only

Microsoft Entra hybrid joined only

Microsoft Entra joined or Microsoft Entra registered only

Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Device2: 

Microsoft Entra joined only

Microsoft Entra registered only

Microsoft Entra hybrid joined only

Microsoft Entra joined or Microsoft Entra registered only

Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Question: 384

You have a Microsoft 365 subscription and use Microsoft Intune.

You need to implement Microsoft Tunnel for Mobile Application Management (MAM) for personal Android devices.

You perform the following actions:

- Configure Microsoft Tunnel for managed devices.
- Validate that user devices meet the prerequisites for Tunnel for MAM.
- Create app configuration policies for Microsoft Defender and Microsoft Edge.

What should you configure next?

- A. an app protection policy
- B. a custom profile for Android Enterprise devices
- C. a Conditional Access policy
- D. a VPN profile for Android Enterprise devices

Answer: A

Question: 385

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains 500 Windows devices enrolled in Microsoft Intune.

You deploy Microsoft Defender for Endpoint.

You need to onboard the devices to Defender for Endpoint. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

From the Microsoft Defender portal, configure the **[answer choice]** Endpoint settings:

	▼
Advanced features	
Device groups	
Intune Permissions	
Onboarding	

From the Microsoft Intune admin center, create:

	▼
A compliance policy	
A configuration profile	
An endpoint detection and response (EDR) policy	
A security baseline profile	

Answer:

Answer Area

From the Microsoft Defender portal, configure the **[answer choice]** Endpoint settings:

▼

Advanced features
Device groups
Intune Permissions
Onboarding

From the Microsoft Intune admin center, create:

▼

A compliance policy
A configuration profile
An endpoint detection and response (EDR) policy
A security baseline profile

Question: 386

HOTSPOT

-

You have a Microsoft 365 subscription that includes Microsoft Intune.

Users have iOS devices that use Microsoft Outlook.

You need to configure Outlook. The solution must meet the following requirements:

- Restrict copy and paste actions from Outlook other apps.
- Enable S/MIME for Outlook.

Which type of policy should you configure for each requirement? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

Restrict copy and paste:

▼

App configuration policy
App protection policy
Compliance policy

Enable S/MIME:

▼

App configuration policy
App protection policy
Compliance policy

Answer:

Answer Area

Restrict copy and paste:

▼

App configuration policy
App protection policy
Compliance policy

Enable S/MIME:

▼

App configuration policy
App protection policy
Compliance policy

Question: 387

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform	Member of
Device1	Windows 11	Group1
Device2	Android	Group1
Device3	iOS	Group1, Group2

All the devices are enrolled in Microsoft Intune.

The devices have apps installed as shown in the following table.

Device	App
Device1	Microsoft Edge, Microsoft Teams
Device2	Microsoft Edge, Microsoft OneDrive
Device3	Microsoft Edge

In Intune, you create an app configuration policy named Policy1 that has the following settings:

- Device enrollment type: Managed apps
- Target policy to: All Microsoft Apps
- Assignments
 - oIncluded groups: Group1
 - oExcluded groups: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Policy1 will apply to Teams on Device1.	<input type="radio"/>	<input type="radio"/>
Policy1 will apply to OneDrive on Device2.	<input type="radio"/>	<input type="radio"/>
Policy1 will apply to Microsoft Edge on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Policy1 will apply to Teams on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Policy1 will apply to OneDrive on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
Policy1 will apply to Microsoft Edge on Device3.	<input type="radio"/>	<input checked="" type="radio"/>